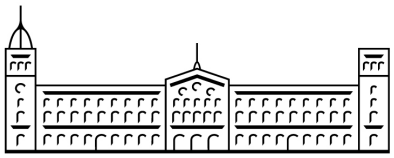

Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques
Universitat de Barcelona

ARITMÈTICA EN L'ANELL DELS QUATERNIONS DE HURWITZ

Adriana Moya Viñas

Directora: Dra. Pilar Bayer
Realitzat al: Departament de Matemàtiques i Informàtica. UB

Barcelona, 27 de juny de 2016

Abstract

This work begins with a brief study of quaternion algebras in order to introduce the division algebra of Hamilton's quaternions. Then we proceed to describe the ring of Hurwitz integers, named after his author, and to study the main properties of it. Finally, using all the previous theory, we prove some results to stress the importance of this ring.

Resum

El treball s'inicia amb un breu estudi de les àlgebres de quaternions, per a així poder introduir el cos dels quaternions de Hamilton. Tot seguit, donem a conèixer l'anell dels enters de Hurwitz, batejat amb el nom del seu creador. Estudiem les seves principals propietats i, finalment, gràcies a aquestes, demostrem alguns resultats que fan palesa la importància d'aquest anell.

What now we see is a shadow of what must come.

Sri Aurobindo, Savitri 1.4

Introducció

El projecte

L'estudi de les àlgebres de quaternions ha donat lloc a molts objectes de la matemàtica moderna, així com les formes modulars i les corbes de Shimura. Tot i així, les àlgebres que han donat lloc a aquests objectes són les que s'anomenen àlgebres indefinides. Nosaltres hem volgut estudiar-ne una de l'altre tipus, les àlgebres definides. D'aquesta n'hem triat una en particular, ben coneguda com els quaternions de Hamilton. Ens hem introduit en un dels seus ordres i hem pogut comprovar que gràcies a aquest ordre es demostren resultats que aparentment no tenen res a veure amb els quaternions. L'objectiu d'aquest treball és fer notar que els ordres en aquests tipus d'àlgebres, les definides, poden donar lloc a resultats no directament relacionats amb aquestes.

Hem realitzat l'estudi sobre l'article *Ueber die Zahlentheorie der Quaternionen* del matemàtic alemany Adolf Hurwitz on presenta un ordre del cos dels Quaternions de Hamilton, actualment anomenat anell d'enters de Hurwitz. Hem volgut estudiarne l'article original per poder trobar quins resultats han quedat dissimulats darrere els estudis més moderns d'aquest anell. L'article original és de l'any 1896, fet que ha provocat un petit canvi en el llenguatge que utilitzem actualment. A continuació mostrarem els exemples més representatius que hem pogut trobar a l'article d'aquest canvi d'època.

Article	Traducció	Significat actual
Permutation	Permutació	Automorfisme
System	Sistema	Conjunt
Substitution	Substitució	Funció
Inversion	Inversió	Antiautomorfisme
Base	Base	Sistema de generadors
Zahlen quaternionen	Quaternió enter	Enter de Hurwitz
Holoedrisch isomorph	Isomorfisme holoèdric	Isomorfisme d'anells

També hem pogut trobar dos casos en què hem notat el canvi d'època en l'estil de les demostracions. El primer cas és en el decurs de la secció 5.4, en el qual per enunciar el teorema d'isomorfia 5.1 primer comprova que $M_2(\mathbb{Z}/m\mathbb{Z})$ és efectivament un anell i després enuncia el teorema simplement demanant que l'aplicació de $\mathcal{O}_H/m\mathcal{O}_H$ a $M_2(\mathbb{Z}/m\mathbb{Z})$ satisfaci, d'una banda que la imatge de $q_1 + q_2$ sigui la suma de les imatges de q_1 i q_2, i d'altra banda que la imatge de q_1q_2 sigui el producte de les imatges de q_1 i q_2. Després, per demostrar el teorema 5.2 defineix un isomorfisme holoèdric, anomenat actualment isomorfisme d'anells. El segon cas

en què hem trobat un petit canvi en el raonament és en la demostració del teorema 6.3. Aquesta prova fa servir l'actualment coneguda com inducció matemàtica, però Hurwitz necessita explicar els raonaments que segueixen aquests tipus de proves.

Estructura de la Memòria

Tot i que l'objectiu del treball és estudiar amb tot detall els resultats que mostra Hurwitz a l'article original, hem trobat oportú conèixer una mica més el que generalitza el cos dels quaternions de Hamilton, és a dir, les àlgebres de quaternions qualssevol. Per aquest motiu, el treball està dividit en parts.

La secció 1 introdueix les àlgebres de quaternions sobre un cos de nombres i la forma nòrmica associada a cada àlgebra. Tal i com mostra el teorema 1.1, l'estudi de la forma nòrmica d'una àlgebra de quaternions és essencial per decidir si l'àlgebra en qüestió és un cos o no. Aquest estudi es complementa amb una brevíssima introducció del símbol de Hilbert i l'enunciat del teorema de Wedderburn (1.2). Tot seguit, es presenten alguns exemples concrets d'àlgebres de quaternions i es distingeix si són cossos o no. La secció 2 es limita a estudiar el cos dels quaternions de Hamilton i els seus automorfismes. Es completa aquesta primera part del treball amb el teorema de Skolem-Noether aplicat a l'àlgebra simple central $\mathbb{H}_{\mathbb{Q}}$ (2.1), i el teorema de Frobenius (2.2).

Tal i com hem dit anteriorment, la part més important del treball està en l'anàlisi de l'article de Hurwitz, que constitueix la segona part del treball. Aquesta té inici amb la definició d'element enter i d'ordre per a qualsevol àlgebra de quaternions. Tot seguit, distingim del conjunt de tots els ordres, el conegut com a *anell dels enters de Hurwitz* $\mathcal{O}_H$. D'aquest anell, estudiem les seves unitats i els seus automorfismes. Val a dir, que tant l'estudi del grup de les unitats com el dels automorfismes està incomplet en el treball de Hurwitz, ja que presenta el conjunt dels seus elements però manca determinar-ne l'estructura. Nosaltres, com es pot veure en els teoremes 3.2 i 3.3, hem determinat l'estructura d'aquests dos grups.

El treball continua amb la divisibilitat en l'anell, les bones propietats del qual fan que poguem definir un algoritme per calcular i programar la divisió entera entre dos quaternions de Hurwitz. D'altra banda, presentem alguns anells quocient que ens donen les eines necessàries per definir els quaternions parells i els quaternions senars, els primaris i els primitius, nocions que són importants més endavant per a la factorització en quaternions primers d'un enter de Hurwitz. Un fet remarcable d'aquesta part del treball és el resultat que mostra el teorema 5.3, que dedueix un isomorfisme entre dos grups finits que, aparentment, no tenen res a veure amb els quaternions. Aquest isomorfisme justifica la importància que poden tenir els ordres de les àlgebres de quaternions en contextos més generals.

Per acabar la segona part del treball, definim els quaternions primers remarcant el fet que els nombres primers de $\mathbb{Z}$ no són primers a $\mathcal{O}_H$, a diferència de certs primers de Gauss. En darrer terme, demostrem que la factorització d'enters de Hurwitz en quaternions primers és possible i en considerem la unicitat. La fem efectiva amb un algoritme programat en la secció 8.

La última part del treball consta de dues aplicacions dels quaternions. D'una banda, s'exposa una bijecció entre l'espai $\mathbb{R}^3$ i els quaternions purs, que permet expressar amb comoditat les rotacions de l'espai a partir d'automorfismes interns de $\mathbb{H}$. D'altra banda, es presenta de forma senzilla un refinament del teorema de Lagrange, que mostra el nombre de maneres en què un nombre enter és expressable com a suma de quatre quadrats. Altre cop, ens hem trobat amb un resultat no directament relacionat amb els quaternions.

Agraïments

Vull agrair especialment a la Dra. Pilar Bayer i Isant per la proposta del tema, totes les hores que m'ha dedicat i les ganes que ha mostrat en tot moment per ajudar-me en els dubtes que han anat sorgint al llarg del treball. També vull fer notar que ha sabut traspassar-me la passió que té per tot el que està relacionat amb aprendre, descobrir i, sobretot, reflexionar sobre les preguntes que sorgeixen. Ha estat una gran tutora i també una gran professora, ja que sense els seus coneixements i el seu interès, molts dels resultats que es veuen en aquest treball estarien incomplerts.

També vull donar les gràcies a totes les persones que m'han donat suport durant aquests mesos, en particular a la meva família i la meva parella pels ànims i la paciència que han tingut al llarg dels meus estudis.

Contingut

1 Àlgebres de quaternions

1.1 Àlgebres de quaternions sobre un cos commutatiu

Definició 1.1. Sigui F un cos commutatiu de característica zero. Definim el conjunt dels *quaternions* $\left(\frac{\alpha,\beta}{F}\right)$ com el F-espai vectorial de dimensió 4 generat pels elements $\{e_0, e_1, e_2, e_3\}$ i dotat d'un producte que segueix les regles següents:

- El producte és bilineal.
- L'element neutre és e_0.
- $e_1^2 = \alpha e_0$,
  $e_2^2 = \beta e_0$,
  $e_1 e_2 = -e_2 e_1 = e_3$.

Observem que amb aquestes tres identitats podem construir la taula següent de multiplicació:

$\cdot$	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	αe_0	e_3	αe_2
e_2	e_2	$-e_3$	βe_0	$-\beta e_1$
e_3	e_3	$-\alpha e_2$	βe_1	$-\alpha\beta e_0$

Nota: La taula indica el producte de l'element de la fila per l'element de la columna. Notem que la taula no és simètrica perquè el producte no és commutatiu.

Amb aquesta taula és fàcil veure que el producte és associatiu. Només s'han de calcular les 27 ternes ordenades i comprovar que:

$$e_i(e_j e_k) = (e_i e_j)e_k, \quad i, j, k \in \{1, 2, 3\}. \tag{1.1}$$

Proposició 1.1. *Siguin F un cos commutatiu i $\alpha, \beta \in F$, aleshores $\left(\frac{\alpha,\beta}{F}\right)$ és una F-àlgebra associativa de dimensió 4.* □

Proposició 1.2. *L'àlgebra de quaternions $\left(\frac{\alpha,\beta}{F}\right)$ és central i té com a centre el cos F.*

Demostració. Considerem un element $q = a + be_1 + ce_2 + de_3$ del centre de $\left(\frac{\alpha,\beta}{F}\right)$, és a dir, q commuta amb qualsevol quaternió de $\left(\frac{\alpha,\beta}{F}\right)$. En particular tenim que

$$qe_1 - e_1 q = 0 \Longrightarrow 2ce_3 + 2\alpha de_2 = 0 \Longrightarrow 2e_3(c + de_1) = 0.$$

Com que e_3 és invertible (en efecte, $e_3 \dfrac{-e_3}{\alpha\beta} = 1$),

$$c + de_1 = 0 \Longrightarrow c = d = 0.$$

Equivalentment,

$$xe_2 + e_2x = 0 \Longrightarrow 2e_3(b + de_2) = 0 \Longrightarrow b = d = 0.$$

Per tant, $q = a$, $a \in F$ i d'aquí obtenim que el centre de $\left(\frac{\alpha,\beta}{F}\right)$ és F. □

Per entendre el resultat següent, recordem que una àlgebra A és simple si no conté ideals bilaterals diferents de $\{0\}$ i A.

Proposició 1.3. *L'àlgebra de quaternions $\left(\frac{\alpha,\beta}{F}\right)$ és una F-àlgebra simple.*

Demostració. Veurem que donat un ideal $\mathfrak{a}$ bilateral no nul de l'àlgebra de quaternions, aquest ideal haurà de ser el total. És suficient veure que $\mathfrak{a}$ conté un element del cos F no nul. Això és perquè si aquest existeix, podem multiplicar-lo pel seu invers (que existeix ja que F és un cos) i així obtenir que $1 \in \mathfrak{a}$.

Sigui $q = a + be_1 + ce_2 + de_3$ un element de $\mathfrak{a}$ no nul. Suposem que almenys un dels tres elements b, c o d són no nuls, ja que si no fos així tindríem que $q = a \in F$ i ja estaríem. Com que $qe_1 - e_1q \in \mathfrak{a}$, tenim que

$$2ce_3 + 2\alpha de_2 \in \mathfrak{a} \Rightarrow (c + de_1)2e_3 \in \mathfrak{a} \Rightarrow c + de_1 \in \mathfrak{a} \Rightarrow ce_2 + de_3 \in \mathfrak{a} \Rightarrow a + be_1 \in \mathfrak{a}.$$

D'altra banda, $qe_2 - e_2q \in \mathfrak{a}$, per tant

$$2\beta de_1 + 2be_3 \in \mathfrak{a} \Rightarrow (b - de_2)2e_3 \in \mathfrak{a} \Rightarrow b - de_2 \in \mathfrak{a} \Rightarrow be_1 + de_3 \in \mathfrak{a} \Rightarrow a + ce_2 \in \mathfrak{a}.$$

Per últim, $qe_3 - e_3q \in \mathfrak{a}$, i per tant tenim que

$$2\beta ce_1 - 2\alpha be_2 \in \mathfrak{a} \Rightarrow 2e_3(ce_2 + be_1) \in \mathfrak{a} \Rightarrow ce_2 + be_1 \in \mathfrak{a} \Rightarrow a + de_3 \in \mathfrak{a}.$$

Sumant aquests tres elements, i restant-li q, tenim que

$$(a + be_1) + (a + ce_2) + (a + de_3) - y = 2a \in \mathfrak{a} \Longrightarrow a \in \mathfrak{a}.$$

Hem trobat que tot element $a \in F$ és tal que $a \in \mathfrak{a}$ i pel raonament que hem mostrat anteriorment, l'ideal $\mathfrak{a}$ és el total. □

Definició 1.2. Sigui $q \in \left(\frac{\alpha,\beta}{F}\right)$, on $q = a + be_1 + ce_2 + de_3$. Definim el seu *conjugat* com

$$\bar{q} = a - be_0 - ce_1 - de_2,$$

i la seva *norma* com

$$N(q) = q\bar{q} = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2.$$

Observació 1. $N(q) \in F$.

Proposició 1.4. *La conjugació és un antiautomorfisme i la norma és multiplicativa.*

Demostració. Si tenim $p = x_0 + x_1e_1 + x_2e_2 + x_3e_3$ i $q = y_0 + y_1e_1 + y_2e_2 + y_3e_3$.

$$\begin{aligned} pq = {} & x_0y_0 + \alpha x_1y_1 + \beta x_2y_2 - \alpha\beta x_3y_3 + (x_0y_1 + x_1y_0 - x_2y_3\beta + x_3y_2\beta)e_1 \\ & + (x_0y_2 + x_2y_0 - \alpha x_3y_1 + \alpha x_1y_3)e_2 + (x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)e_3. \end{aligned}$$

Aleshores,

$$\begin{aligned} \overline{pq} = {} & x_0y_0 + \alpha x_1y_1 + \beta x_2y_2 - \alpha\beta x_3y_3 + (-x_0y_1 - x_1y_0 + x_2y_3\beta - x_3y_2\beta)e_1 \\ & + (-x_0y_2 - x_2y_0 + \alpha x_3y_1 - \alpha x_1y_3)e_2 + (-x_0y_3 - x_3y_0 - x_1y_2 + x_2y_1)e_3, \end{aligned}$$

$$\begin{aligned} \bar{q}\bar{p} &= (y_0 - y_1e_1 - y_2e_2 - y_3e_3)(x_0 - x_1e_1 - x_2e_2 - x_3e_3) \\ &= y_0x_0 + y_1x_1\alpha + y_2x_2\beta - \alpha\beta y_3x_3 + (-y_0x_1 - y_1x_0 - y_2x_3\beta + y_3x_2\beta)e_1 \\ &\quad + (-y_0x_2 - y_2x_0 - \alpha y_3x_1 + \alpha y_1x_3)e_2 + (-y_0x_3 - y_3x_0 + y_1x_2 - y_2x_1)e_3. \end{aligned}$$

Efectivament, $\overline{pq} = \bar{q}\bar{p}$.

Si $p, q \in \left(\frac{\alpha,\beta}{F}\right)$,

$$N(pq) = pq\overline{pq} = pq\bar{q}\bar{p} = pN(q)\bar{p} = N(q)p\bar{p} = N(q)N(p).$$

□

Notem que l'algebra $\left(\frac{\alpha,\beta}{F}\right)$ no és, en general, un cos. Però tenim alguns resultats que ens ajuden a veure quines àlgebres són cossos i quines no ho són.

Lema 1.1. *Si l'equació $x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 = 0$ no té solucions no trivials en F, aleshores l'àlgebra $\left(\frac{\alpha,\beta}{F}\right)$ és un cos.*

Demostració. Si l'equació no té solucions, aleshores per a tot $q \neq 0$ es té que $N(q) \neq 0$. Sigui q un quaternió, definim l'element q^{-1} com:

$$q^{-1} = \frac{\bar{q}}{N(q)}. \tag{1.2}$$

Aleshores és cert que $qq^{-1} = q\frac{\bar{q}}{N(q)} = \frac{q\bar{q}}{N(q)} = 1 = \frac{\bar{q}q}{N(q)} = q^{-1}q$. Per tant, tot element no nul té invers. □

En cas contrari, l'algebra no serà un cos perquè no podem definir l'element invers dels divisors de 0. Però tenim un resultat que caracteritza aquests tipus d'àlgebres.

Teorema 1.1. *Si l'equació*

$$x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 = 0 \tag{1.3}$$

té alguna solució no trivial en F, i $\alpha, \beta \neq 0$, aleshores l'àlgebra $\left(\frac{\alpha,\beta}{F}\right)$ és isomorfa a l'àlgebra de matrius $M_2(F)$.

Procedirem a la demostració del teorema després de veure dos resultats necessaris per a la seva prova.

Lema 1.2. *Si l'equació $\alpha x^2 + \beta y^2 = 1$ té alguna solució no trivial, l'àlgebra $\left(\frac{\alpha,\beta}{F}\right)$ és isomorfa a $M_2(F)$.*

Demostració. Siguin x, y les solucions de l'equació, definim els següents elements:

$$\begin{aligned}\varepsilon_1 &= xe_1 + y,\\ \varepsilon_2 &= e_3,\\ \varepsilon_3 &= \epsilon_1\epsilon_2 = -\beta y e_1 + \alpha x e_2.\end{aligned}$$

Aleshores $\{1, \epsilon_1, \epsilon_2, \epsilon_3\}$ és una base de l'algebra de quaternions $\left(\frac{1,-\alpha\beta}{F}\right)$. En efecte, $\epsilon_1^2 = 1$, $\epsilon_2^2 = -\alpha\beta$, $\epsilon_1\epsilon_2 = \epsilon_3 = -\epsilon_2\epsilon_1$.

Amb l'isomorfisme següent, tenim que aquesta àlgebra (i, en particular, $\left(\frac{\alpha,\beta}{F}\right)$) són isomorfes a $M_2(F)$:

$$\begin{array}{rcl}\left(\dfrac{1,-\alpha\beta}{F}\right) & \longrightarrow & M_2(F)\\ 1 & \longmapsto & \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\\ \varepsilon_1 & \longmapsto & \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)\\ \varepsilon_2 & \longmapsto & \left(\begin{smallmatrix}0&1\\-\alpha\beta&0\end{smallmatrix}\right)\\ \varepsilon_3 & \longmapsto & \left(\begin{smallmatrix}0&-1\\-\alpha\beta&0\end{smallmatrix}\right).\end{array}$$

□

Lema 1.3. *Si l'equació $\alpha x^2 + \beta y^2 - z^2 = 0$ té alguna solució no trivial, l'àlgebra $\left(\frac{\alpha,\beta}{F}\right)$ és isomorfa a $M_2(F)$.*

Demostració. Si $z \neq 0$ aleshores aplicant el lema 1.2 ja estem. En cas contrari, tindríem que $-\alpha\beta$ es un quadrat a F i per tant l'àlgebra és isomorfa a $\left(\frac{1,-\alpha\beta}{F}\right)$. Amb el mateix isomorfisme que hem utilitzat en el cas anterior, l'àlgebra és isomorfa a $M_2(F)$. □

Demostració. Procedim a la demostració del Teorema 1.1

Sigui x_0, x_1, x_2, x_3 una solució no trivial en F, aleshores si $x_3 = 0$ estem en el cas del lema 1.3 per tant, ja estem.

Suposem ara $x_3 \neq 0$. Aleshores, siquin $q = x_0 + x_1e_1 + x_2e_2 + x_3e_3$ i $p = x_2 - x_3e_3$. Tenim que p és invertible ja que té norma $x_2^2 - \alpha x_3^2 \neq 0$. Per tant,

$$pq = x_2x_0 - \alpha x_1x_3 + (x_1x_2 - x_0x_3)e_1 + (x_2^2 - \alpha x_3^2)e_2 \neq 0.$$

I, a més, pq té norma nul·la ja que $N(q) = 0$. Per tant,

$$N(pq) = (x_0x_2 - \alpha x_1x_3)^2 - \alpha(x_1x_2 - x_0x_3)^2 - \beta(x_2^2 - \alpha x_3^2) = 0.$$

Observem que tornem a estar en les hipòtesis del lema 1.3 i, per tant, l'àlgebra dels quaternions és isomorfa a $M_2(F)$.

□

1.2 Àlgebres de quaternions sobre $\mathbb{R}$

L'àlgebra de quaternions que estudiarem sobre $\mathbb{R}$ és coneguda com els *Quaternions de Hamilton*. Formalment, posem que l'àlgebra dels quatenrnions de Hamilton és $\mathbb{H} := \left(\frac{-1,-1}{\mathbb{R}}\right)$. Pel lema 1.1, si veiem que l'equació

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$$

no té solucions a $\mathbb{R}$, aleshores deduirem que l'àlgebra dels quaternions sobre $\mathbb{R}$ és un cos. Veure que l'equació no té solucions és trivial ja que els nombres $x_i \in \mathbb{R}$ tenen quadrat positiu i, per tant,

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0 \Longleftrightarrow x_0 = x_1 = x_2 = x_3 = 0.$$

A partir d'aquest moment, anomenarem $\mathbb{H}$ el cos dels quaternions de Hamilton.

1.3 Teorema de Wedderburn

Tot i poder classificar les àlgebres segons l'existència de solucions de l'equació 1.3, no sempre és trivial trobar-les o demostrar la seva inexistència. Per exemple, per saber si l'àlgebra $\left(\frac{3,-1}{\mathbb{Q}}\right)$ és un cos o no hauríem de trobar les solucions (o demostrar que no en té) de l'equació $x^2 - 3y^2 + z^2 - 3t^2 = 0$, i com que estem a $\mathbb{Q}$ i 3 no és un quadrat a $\mathbb{Q}$ no és fàcil buscar-les (de fet, més endavant veurem que aquesta àlgebra és un cos). Per poder classificar les àlgebres d'una forma més eficaç enunciarem els següents resultats, que no demostrarem, ja que depassen l'objectiu del treball.

Teorema 1.2 (Wedderburn)**.** *Sigui A una àlgebra simple sobre un cos F, aleshores $A \cong M_n(D)$ on D és un cos no commutatiu.* □

Corol·lari 1.1. *Sigui $\left(\frac{\alpha,\beta}{F}\right)$ l'àlgebra dels quaternions sobre F, aleshores o bé*

$$\left(\frac{\alpha,\beta}{F}\right) \cong M_2(F)$$

o bé,

$$\left(\frac{\alpha,\beta}{F}\right) \quad \textit{és un cos no commutatiu.}$$

Definició 1.3. Siguin a, b no nuls i $\left(\frac{\alpha,\beta}{F}\right)$ l'àlgebra dels quaternions. Definim el *símbol de Hilbert* sobre F de la parella (α, β) com:

$$(\alpha,\beta)_F = \begin{cases} 1 & \text{si } \left(\frac{\alpha,\beta}{F}\right) \cong M_2(F), \\ -1 & \text{si } \left(\frac{\alpha,\beta}{F}\right) \text{ és un cos no commutatiu.} \end{cases} \tag{1.4}$$

1.4 Àlgebres de quaternions sobre $\mathbb{Q}$

Exemple 1. $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ és un cos (*Cos dels quaternions racionals*). En efecte, l'equació

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$$

no té solucions no trivials a $\mathbb{Q}$ i pel lema 1.1, $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ és un cos.

Exemple 2. $\left(\frac{1,b}{\mathbb{Q}}\right)$ no és un cos ja que l'equació $x^2 - y^2 - bz^2 + bt^2 = 0$ té les solucions següents:

$$\begin{aligned} 2x &= (b+1)z + (1-b)t, \\ 2y &= (b-1)z + (-b-1)t, \end{aligned}$$

per a tot $z, t \in \mathbb{Q}$. I pel teorema 1.1, l'àlgebra $\left(\frac{1,b}{\mathbb{Q}}\right)$ és isomorfa a $M_2(\mathbb{Q})$.

Com ja hem observat, en general l'equació $x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 = 0$ no és fàcil de resoldre a $\mathbb{Q}$. Per aquest motiu, farem efectiu el càlcul del símbol de Hilbert pels racionals, i així podrem determinar si una àlgebra de quaternions racionals és un cos o no.

Escrivim $(\alpha, \beta)_\infty$ si $F = \mathbb{R}$, el cos dels nombres reals, i $(\alpha, \beta)_p$ si $F = \mathbb{Q}_p$, el cos dels nombres p-àdics. El càlcul del símbol de Hilbert en el cas $F = \mathbb{R}$ és:

$$(\alpha, \beta)_\infty = \begin{cases} 1 & \text{si } \alpha > 0 \text{ o bé } \beta > 0, \\ -1 & \text{si } \alpha < 0 \text{ i } \beta < 0. \end{cases}$$

I en el cas $F = \mathbb{Q}_p$, si

$$\begin{aligned} \alpha &= p^a u \quad \text{amb } p \nmid u \\ \beta &= p^b v \quad \text{amb } p \nmid v \end{aligned}$$

Aleshores tenim que:

$$(\alpha, \beta)_p = \begin{cases} (-1)^{ab\varepsilon(p)} \left(\frac{u}{p}\right)^b \left(\frac{v}{p}\right)^a & \text{si } p \neq 2, \\ (-1)^{\varepsilon(u)\varepsilon(v) + a\omega(v) + b\omega(u)} & \text{si } p = 2. \end{cases}$$

amb $\varepsilon(z) = \dfrac{z-1}{2}$, $\omega(z) = \dfrac{z^2-1}{8}$. On $\left(\dfrac{u}{p}\right)$ denota el símbol de Legendre.

Ara bé pel cas $F = \mathbb{Q}$ tenim el resultat següent:

Teorema 1.3 (Principi local global)**.** *Donats $\alpha, \beta \in \mathbb{Q}^*$, es té que*

$$(\alpha, \beta)_\mathbb{Q} = 1 \iff \begin{cases} (\alpha, \beta)_\infty = 1, \\ (\alpha, \beta)_p = 1, \quad \textit{per a tot } p \textit{ primer.} \end{cases} \tag{1.5}$$

Observem que el símbol de Hilbert $(\alpha, \beta)_p$ sol pot ser -1 en un nombre finit de primers p (més concretament, els que divideixen α o β). I això ens permet calcular, amb un nombre finit de passos, el símbol de Hilbert $(\alpha, \beta)_{\mathbb{Q}}$. En efecte, si p no divideix α ni β, aleshores $a = 0$ i $b = 0$, i tenim que $(\alpha, \beta)_p = 1$ per a tot p primer $p \neq 2$. Per tant, els únics primers p tals que el símbol de Hilbert $(\alpha, \beta)_p$ pot ser -1 són els que divideixen α o β.

Ara ja sóm capaços de determinar si una àlgebra de quaternions sobre $\mathbb{Q}$ és cos o no, per mitjà del criteri 1.4.

Exemple 3. L'àlgebra $\left(\frac{3,-1}{\mathbb{Q}}\right)$ és un cos. Vegem-ho:

El símbol de Hilbert $(3, -1)_\infty = 1$ ja que $3 > 0$.

Per a $p = 3$ tenim que:

$$3 = 3^1 \cdot 1 \Longrightarrow a = 1 \text{ i } u = 1,$$

$$-1 = 3^0 \cdot (-1) \Longrightarrow b = 0 \text{ i } v = -1.$$

Per tant:

$$(3, -1)_3 = (-1)^0 \left(\frac{1}{3}\right)^0 \left(\frac{-1}{3}\right)^1 = \left(\frac{2}{3}\right) = -1.$$

Com que hem trobat un p primer tal que $(3, -1)_p \neq 1$, pel principi local global, $(a, b) = -1$. I, per tant, l'àlgebra $\left(\frac{3,-1}{\mathbb{Q}}\right)$ és un cos no commutatiu. Notem que, també, $(3, -1)_2 = -1$.

Exemple 4. L'àlgebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ és un cos. Vegem-ho:

Sigui $p \neq 2$, com que p no divideix -1 tenim que $a, b = 0$ i per tant $(-1, -1)_p = 1$.

D'altra banda, per a $p = 2$ tenim que $u = -1$ i $v = -1$. Per tant,

$$(-1, -1)_2 = (-1)^{1-0-0} = -1.$$

I, a més,

$$(-1, -1)_\infty = -1.$$

Com que hem trobat que $(-1, -1)_\infty \neq 1$ i $(-1, -1)_2 \neq 1$, pel principi local global tenim que $(-1, -1)_{\mathbb{Q}} = -1$. I per tant l'algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ és un cos no commutatiu.

2 El cos dels quaternions reals

2.1 El cos $\mathbb{H}$ dels quaternions reals

Definició 2.1. Denotem per $\mathbb{H}$ el cos dels *quaternions reals* (o quaternions de Hamilton) l'àlgebra $\left(\frac{-1,-1}{\mathbb{R}}\right)$ definida en la secció anterior com el $\mathbb{R}$-espai vectorial de dimensió 4 generat per $\{1, i, j, k\}$ tal que:

- El producte és bilineal.
- L'element neutre és 1.
- $i^2 = -1$,
  $j^2 = -1$,
  $i \cdot j = -j \cdot i = k$.

D'on podem deduir la taula de multiplicació següent (on l'ordre del producte és fila per columna):

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Tots els conceptes definits a les àlgebres de quaternions els tenim en aquest cas particular, i són els següents.

Definició 2.2. Donat un quaternio real $q = a + bi + cj + dk$ definim el *conjugat* de q per

$$\bar{q} = a - bi - cj - dk$$

i la seva *norma* com

$$N(q) = q\bar{q} = a^2 + b^2 + c^2 + d^2.$$

A més, direm que q és un quaternió de *part real* a. I si $a = 0$ direm que q és un *quaternió pur*.

Notem que la norma és multiplicativa, ja ho hem vist per a les àlgebres de quaternions en la secció primera, i $\mathbb{H}$ n'és un cas particular.

Observació 2. Efectivament $\mathbb{H}$ és un cos, ja que l'equació $x_0^2+x_1^2+x_2^2+x_3^2 = 0$ no té solucions no trivials a $\mathbb{R}$. Pel lema 1.1, $\mathbb{H}$ és un cos amb element invers $q^{-1} = \dfrac{\bar{q}}{N(q)}$.

2.2 Automorfismes de $\mathbb{H}$

Una vegada hem vist el cos dels quaternions, hem d'estudiar les aplicacions que tenen bones propietats en aquest cos. Fins i tot veurem que hi ha subcossos de $\mathbb{H}$ que són invariants per aquest tipus d'aplicacions.

Definició 2.3. Diem que una aplicació no nul·la

$$f : \mathbb{H} \longrightarrow \mathbb{H}$$

és un *automorfisme* del cos dels quaternions si

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \text{ per a tot } a, b \in \mathbb{H}.$$

Proposició 2.1. *Tot automorfisme de $\mathbb{H}$ deixa fix $\mathbb{Q}$ i, per tant, tot automorfisme de $\mathbb{H}$ ho és de $\mathbb{Q}$-àlgebres.*

Demostració. Observem primer que $f(1) = 1$. En efecte, per a tot $x \in \mathbb{H}$, es té que

$$f(x) = f(1 \cdot x) = f(1)f(x).$$

Sigui $p \in \mathbb{N}$ aleshores

$$f(p) = f(1 + 1 + ... + 1 + 1) = pf(1) = p.$$

D'altra banda, observem que si $q \neq 0$ aleshores $f\left(\frac{1}{q}\right) = \frac{1}{q}$ ja que

$$f\left(\frac{1}{q}\right) \cdot q = f\left(\frac{1}{q}\right) \cdot f(q) = f\left(\frac{q}{q}\right) = f(1) = 1.$$

Aleshores, sigui $\frac{p}{q} \in \mathbb{Q}$, $\text{mcd}(p, q) = 1$ tenim que:

$$f\left(\frac{p}{q}\right) = f\left(p\frac{1}{q}\right) = f(p)f\left(\frac{1}{q}\right) = \frac{p}{q}.$$

□

Proposició 2.2 (Propietats)**.** *Sigui f un automorfisme del cos dels quaternions,*

1. $f(0) = 0$.
2. $f(a) = f(b) \Longleftrightarrow a = b$.

Demostració. 1. Sigui $x \in \mathbb{H}$ qualsevol, aleshores

$$f(0) = f(x - x) = f(x) + f(-x) = f(x) - f(x) = 0.$$

2. $f(a) = f(b) \Leftrightarrow f(a) - f(b) = 0 \Leftrightarrow f(a - b) = 0 \Leftrightarrow a - b = 0 \Leftrightarrow a = b$.

□

Definició 2.4. Diem que una aplicació no nul·la

$$f : \mathbb{H} \longrightarrow \mathbb{H}$$

és un *antiautomorfisme* del cos dels quaternions si

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(b)f(a), \text{ per a tot } a, b \in \mathbb{H}.$$

Les propietats que hem vist amb els automorfismes de $\mathbb{H}$ també són certes en aquest cas. I, a més, podem relacionar els automorfismes i els antiautomorfismes de $\mathbb{H}$ amb el resultat següent.

Proposició 2.3. *Tot antiautomorfisme es pot posar com la composició d'un automorfisme i la aplicació conjugació.*

Demostració. Sigui f un antiautomorfisme, definim $g = \overline{f(a)}$. Aleshores g és un automorfisme de $\mathbb{H}$ i $f = \sigma \circ g$ (on σ és la cojugació).

$$g(a+b) = \overline{f(a+b)} = \overline{f(a) + f(b)} = \overline{f(a)} + \overline{f(b)} = g(a) + g(b),$$
$$g(ab) = \overline{f(ab)} = \overline{f(b)f(a)} = \overline{f(a)} \cdot \overline{f(b)} = g(a)g(b).$$

□

Com que hi ha una correspondència bijectiva entre el conjunt dels automorfismes i el dels antiautomorfismes, a partir d'ara només treballarem amb els automorfismes, i tots els resultats que veiem es poden estendre als antiautomorfismes de manera directa utilitzant la conjugació. Vegem alguns exemples d'automorfismes.

Exemple 5. Sigui $q \in \mathbb{H}$, aleshores l'aplicació

$$\begin{aligned} f : \quad & \mathbb{H} \longrightarrow \mathbb{H} \\ & r \longmapsto qrq^{-1} \end{aligned}$$

és un automorfisme. En efecte,

$$q(a+b)q^{-1} = qaq^{-1} + qbq^{-1},$$
$$q(ab)q^{-1} = qaq^{-1} \cdot qbq^{-1}.$$

Exemple 6. Si α, β, γ és una permutació de i, j, k, aleshores l'aplicació

$$\begin{aligned} f : \quad & \mathbb{H} \longrightarrow \mathbb{H} \\ & i \longmapsto \pm\alpha, \\ & j \longmapsto \pm\beta, \\ & k \longmapsto \pm\gamma, \end{aligned}$$

de tal manera que $\pm\alpha \cdot \pm\beta \cdot \pm\gamma = -1$, és un automorfisme.

D'aquests automorfismes n'hi ha 24, ja que podem fer 6 permutacions de i, j, k i d'aquestes tenim 8 possibles canvis de signe. Per tant tenim 48 possibilitats i li traiem les que

$$\pm\alpha \cdot \pm\beta \cdot \pm\gamma = 1$$

obtenint així 24 possibles automorfismes d'aquest tipus.

Es pot veure que els automorfismes del tipus de l'exemple 6 estan continguts en els del tipus de l'exemple 5. No ho veurem en general però farem un exemple.

Exemple 7. Cosiderem l'aplicació definida per:

$$\begin{pmatrix} i & j & k \\ j & i & -k \end{pmatrix}$$

Efectivament $ij(-k) = -1$, per tant l'aplicació

$$\begin{array}{rcl} f: & \mathbb{H} \longrightarrow & \mathbb{H} \\ a+bi+cj+dk & \longmapsto & a+ci+bj-dk \end{array}$$

és un automorfisme.

Notem que f es pot escriure també com $f(q) = (\frac{i}{2}+\frac{j}{2}) \cdot q \cdot (\frac{i}{2}+\frac{j}{2})^{-1}$. En efecte,

$$(\frac{i}{2}+\frac{j}{2})^{-1} = -i-j \Longrightarrow (\frac{i}{2}+\frac{j}{2}) \cdot (a+bi+cj+dk) \cdot (-i-j) = a+ci+bj-dk.$$

Un cop vist que aquests automorfismes que permuten i, j, k estan inclosos als automorfismes de la forma $q(\ )q^{-1}$ per a un cert q, és natural pensar que tots els autormorfismes de $\mathbb{H}$ podrien ser d'aquesta forma, però això no és cert si no restringim l'espai de sortida d'aquests autormorfismes.

Sigui $\mathbb{H}_{\mathbb{Q}} \subseteq \mathbb{H}$ el cos dels *quaternions racionals*, és a dir $\mathbb{H}_{\mathbb{Q}} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$. Aleshores definim els automorfismes de $\mathbb{H}_{\mathbb{Q}}$ de la mateixa manera:

$$f : \mathbb{H}_{\mathbb{Q}} \longrightarrow \mathbb{H}_{\mathbb{Q}}$$

tal que

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad \text{per a tot } a, b \in \mathbb{H}_{\mathbb{Q}}.$$

En aquest cos, tot automorfisme és intern, és a dir es pot posar en la forma $q(\ )q^{-1}$ per a un cert $q \in \mathbb{H}_{\mathbb{Q}}$, $q \neq 0$. Vegem-ho:

Lema 2.1. *Dues solucions en $\mathbb{H}_{\mathbb{Q}}$ de l'equació $X^2 + 1 = 0$ són conjugades. És a dir, donat α un quaternió tal que $\alpha^2 = -1$, aleshores existeix un altre quaternió q que satisfà*

$$\alpha = qiq.^{-1}.$$

Demostració. Siguin b un quaternió no nul i

$$c = \alpha b - bi. \tag{2.1}$$

Si $c = 0$ aleshores $\alpha b = bi \Longrightarrow \alpha = bib^{-1} \Longrightarrow q = b$.

Suposem ara que $c \neq 0$. Multipliquem per α l'equació 2.1 i obtenim

$$\alpha c = \alpha^2 b - \alpha bi = -b - \alpha bi = (\alpha b - bi)(-i) = c(-i) \Rightarrow ci = -\alpha c.$$

Multiplicant per j obtenim la relació següent:

$$cij = -\alpha cj \Rightarrow \alpha cj = -cij = cji.$$

Aleshores, prenent $q = cj$ obtenim que $\alpha(cj) = (cj)i \Longrightarrow \alpha = (cj)i(cj)^{-1}$.

□

Teorema 2.1 (Skolem-Noether)**.** *Tot automorfisme f de $\mathbb{H}_{\mathbb{Q}}$ es pot escriure com un automorfisme intern $q(\ )q^{-1}$, per a un cert $q \in \mathbb{H}_{\mathbb{Q}}$.*

Demostració. Considerem un automorfisme $f : \mathbb{H}_{\mathbb{Q}} \longrightarrow \mathbb{H}_{\mathbb{Q}}$. Com que es manté la propietat 2.1, tenim que el cos $\mathbb{Q}$ és fix per f. Per provar el teorema és suficient veure que existeix un $q \in \mathbb{H}_{\mathbb{Q}}$ tal que

$$\begin{aligned} f(i) &= qiq^{-1}, \\ f(j) &= qjq^{-1}, \\ f(k) &= qkq^{-1}. \end{aligned} \tag{2.2}$$

ja que, per tant, si $r \in \mathbb{H}_{\mathbb{Q}}$, amb $r = a + bi + cj + dk$, és clar que

$$f(r) = a + bf(i) + cf(j) + df(k) = q(a + bi + ck + dk)q^{-1} = qrq^{-1}.$$

Definim $\alpha = f(i), \beta = f(j), \gamma = f(k)$. Aleshores,

$$\alpha^2 = f(i^2) = f(-1) = -1, \quad \beta^2 = -1, \quad \gamma^2 = -1.$$

Pel lema anterior, existeix $q_1 \in \mathbb{H}_{\mathbb{Q}}$ tal que $\alpha = q_1 i q_1^{-1}$.

Siguin

$$\begin{aligned} \alpha_1 &= q_1^{-1}\alpha q_1 = i, \\ \beta_1 &= q_1^{-1}\beta q_1, \\ \gamma_1 &= q_1^{-1}\gamma q_1. \end{aligned} \tag{2.3}$$

Si $\beta_1 = j$ ja estem, ja que

$$j = q_1^{-1}\beta q_1 \Longrightarrow \beta = q_1 j q_1^{-1},$$

$$q_1 k q_1^{-1} = q_1 i q_1^{-1} q_1 j q_1^{-1} = \alpha\beta = f(i)f(j) = f(ij) = f(k) = \gamma \Longrightarrow \gamma = q_1 k q_1^{-1}.$$

Per tant, per a $q = q_1$ se satisfan les equacions 2.2 i tenim que $f(r) = q_1 r q_1^{-1}$.

Suposem ara que $\beta_1 \neq j$. Definim q_2 com

$$q_2 = bk - i = -(\beta_1 j + 1)i.$$

Amb uns càlculs es pot comprovar que es tenen les igualtats següents:

$$\begin{aligned} q_2 i &= a q_2, \\ q_2 j &= b q_2, \\ q_2 k &= c q_2. \end{aligned}$$

Per tant, sigui $q = q_1 q_2$, tenim que

$$\begin{aligned} \alpha = &\quad qiq^{-1}, \\ \beta = &\quad qjq^{-1}, \\ \gamma = &\quad qkq^{-1}. \end{aligned} \tag{2.4}$$

Vegem-ho.

- $\alpha = qiq^{-1}$ Utilitzant que $\alpha = q_1\alpha_1 q_1^{-1}$ i $\alpha_1 = q_2 i q_2^{-1}$ obtenim:

$$\alpha = q_1\alpha_1 q_1^{-1} = q_1 q_2 i q_2^{-1} q_1^{-1} = qiq^{-1}.$$

- $\beta = qjq^{-1}$
  Utilitzant que $\beta = q_1\beta_1 q_1^{-1}$ i $\beta_1 = q_2 j q_2^{-1}$ obtenim:

$$\beta = q_1\beta_1 q_1^{-1} = q_1 q_2 j q_2^{-1} q_1^{-1} = qjq^{-1}.$$

- $\gamma = qkq^{-1}$
  Utilitzant que $\gamma = q_1\gamma_1 q_1^{-1}$ i $\gamma_1 = q_2 k q_2^{-1}$ obtenim:

$$\gamma = q_1\gamma_1 q_1^{-1} = q_1 q_2 k q_2^{-1} q_1^{-1} = qkq^{-1}.$$

Per tant, per a $q = q_1 q_2$ se satisfan les equacions 2.2 i tenim que $f(r) = qrq^{-1}$. □

El resultat que acabem de veure és el que presenta Hurwitz en el seu article original, però no és res més que un cas particular del teorema de Skolem-Noether en el qual es demostra que si R és una Z-àlgebra central simple, aleshores tot automorfisme que deixa invariant Z, és intern. Hurwitz demostra el cas particular en què l'àlgebra central simple és una $\mathbb{Q}$-àlgebra de quaternions. Efectivament, ja hem vist que les àlgebres de quaternions tenen centre $Z = \mathbb{Q}$ i tots els autormorfismes deixen fix $\mathbb{Q}$. Per tant, les hipòtesis del teorema de Skolem-Noether se satisfan i el resultat de Hurwitz és un cas previ del que va ser Skolem-Noether.

2.3 Teorema de Frobenius

Hamilton, en la seva recerca dels quaternions, volia estendre els nombres complexos afegint un segon element imaginari j i crear un cos format per ternes de la forma $a + bi + cj$. Va poder sumar-les i restar-les pero quan va intentar multiplicar-les va veure que necessitava un tercer element que va anomenar $k := ij = -ij$. Així va sorgir el primer cos no commutatiu sobre $\mathbb{R}$. És natural fer-se la mateixa pregunta que va plantejar Hamilton amb els nombres complexos, i intentar estendre el cos dels quaternions reals a un cos no commutatiu sobre $\mathbb{R}$ de dimensió més gran.

Doncs aquesta pregunta la va respondre Frobenius l'any 1878 veient que no hi ha cossos de dimensió finita sobre $\mathbb{R}$ i amb $\mathbb{R}$ dins del seu centre.

Teorema 2.2 (Frobenius)**.** *Sigui K un cos i Z el seu centre. Suposem que $\mathbb{R} \subseteq Z$ i que $dim_{\mathbb{R}} K$ és finita. Aleshores $K \cong \mathbb{R}$, $\mathbb{C}$ ó $\mathbb{H}$.*

Demostració. Si el cos K és commutatiu aleshores $K = \mathbb{R}$ o $K = \mathbb{C}$. En efecte, si K és commutatiu aleshores $K/\mathbb{R}$ és una extensió algebraica i com que $\mathbb{C}$ és un cos algebraicament tancat, per força $K \subseteq \mathbb{C}$. Així, suposem que K no és commutatiu.

Com que $\mathbb{R} \subsetneq K$, considerem $x \in K \backslash \mathbb{R}$ i l'extensió $\mathbb{R}(x)$. Aleshores, $\dim_{\mathbb{R}} \mathbb{R}(x) < \infty$ i $\mathbb{R} \subsetneq \mathbb{R}(x)$. Observem també que $\mathbb{R}(x)$ és commutatiu ja que x commuta amb qualsevol element de $\mathbb{R}$. Al ser $\mathbb{R}(x)$ un cos commutatiu de dimensió finita sobre $\mathbb{R}$, tenim que $\mathbb{R}(x) \cong \mathbb{C}$.

Sigui $e_1 \in \mathbb{R}(x)$, $e_1^2 = -1$ i tal que $\mathbb{R}(x) = \mathbb{R}(e_1)$. Aleshores $\mathbb{R}(e_1)$ és un subcos de K commutatiu maximal ja que és algebraicament tancat. Per tant, tot element de K que commuti amb e_1 ha de caure a $\mathbb{R}(e_1)$.

Sigui $y \in K \setminus \mathbb{R}(e_1)$, posem

$$z = ye_1 - e_1 y.$$

És clar que $z \neq 0$ ja que $y \notin \mathbb{R}(e_1)$, i no commuta amb e_1. A més,

$$\begin{aligned} e_1 z &= e_1 y e_1 + y, \\ z e_1 &= -y - e_1 y e_1, \end{aligned} \tag{2.5}$$

així $ze_1 = -e_1 z \neq 0$ i $z \notin \mathbb{R}(e_1)$.

Com hem fet abans amb x, $\mathbb{R}(z) \cong \mathbb{C}$. Per tant tenim dos extensions simples de $\mathbb{R}$ diferents i podem afirmar que

$$\mathbb{R}(e_1) \cap \mathbb{R}(z) = \mathbb{R}.$$

Volem veure que K és isomorf a $\mathbb{H}$, i per tant hem de trobar dos elements e_2 i e_3 de quadrat -1. De moment sabem que $z \notin \mathbb{R}(e_1)$, per tant:

$$ze_1 = -e_1 z \Longrightarrow z^2 e_1 = -z e_1 z = e_1 z^2 \Longrightarrow z^2 \in \mathbb{R}(e_1),$$

$$\begin{cases} z^2 \in \mathbb{R}(z) \\ z^2 \in \mathbb{R}(e_1) \end{cases} \Longrightarrow z^2 \in \mathbb{R}.$$

Suposem que $z^2 = a$ amb $a \in \mathbb{R}, a > 0$. Aleshores, $(z - \sqrt{a})(z + \sqrt{a})$ seria un divisor de zero. Així, $z^2 = a, a < 0$.

Posem,

$$e_2 = \frac{z}{\sqrt{-a}}$$

i e_2 se satisfà que $e_2^2 = -1$ i $e_1 e_2 = -e_2 e_1$.

Sigui

$$e_3 = e_1 e_2.$$

Aleshores els elements e_1, e_2, e_3 satisfan la taula de multiplicació dels quaternions i, j, k. Per tant els elements $1, e_1, e_2, e_3$ generen un subcòs K' de K isomorf a $\mathbb{H}$.

Ara només resta veure que $K' = K$. Suposem que $K' \subsetneq K$.

Sigui $u \in K \setminus K'$, posem

$$v = ue_1 - e_1u$$

aleshores $v \neq 0$ ja que $u \notin K'$ i per tant $u \notin \mathbb{R}(e_1)$. A més, $v^2 = b \in \mathbb{R}, b < 0$ (pel mateix motiu que $z^2 = a, a < 0$).

Sigui

$$e_4 = \frac{v}{\sqrt{-b}}$$

aleshores $e_4^2 = -1$ i $e_4e_1 = -e_1e_4$. Així $e_4 \notin \mathbb{R}(e_1)$.

D'altra banda, tenim que $K' \supseteq \mathbb{R}(e_1, u) \cap K' \supseteq \mathbb{R}(e_1)$ i $[K' : \mathbb{R}(e_1)] = 2$, per tant

$$L := \mathbb{R}(e_1, u) \cap K' = \mathbb{R}(e_1).$$

Com que $e_4 \in \mathbb{R}(e_1, u)$ i $e_4 \notin \mathbb{R}(e_1)$, aleshores $e_4 \notin K'$ i en particular $e_2e_4 \notin K'$. Però,

$$e_1(e_2e_4) = -(e_2e_1)e_4 = -e_2(e_1e_4) = e_2(e_4e_1) = (e_2e_4)e_1.$$

Com que $\mathbb{R}(e_1)$ és subcòs commutatiu maximal de K, tot element que commuta amb e_1 ha de pertànyer a $\mathbb{R}(e_1)$ i aleshores

$$e_2e_4 \in \mathbb{R}(e_1) \Longrightarrow e_2e_4 \in K'$$

Contradicció ja que teníem que $e_2e_4 \notin K'$.

□

Tot i que el teorema de Frobenius ens assegura que no és possible estendre el cos dels quaternions reals de manera associativa, es va continuar amb la recerca d'un cos de dimensió finita que generalitzés els quaternions. Així, Arthur Cayley va publicar l'any 1845 un article on anunciava l'existència d'un cos no commutatiu i no associatiu, actualment anomenat com el cos dels octonions $\mathbb{O}$ (o nombres de Cayley). Com a espai vectorial sobre $\mathbb{R}$, està generat per 8 elements $\{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ dels quals per a tot i es té que $e_i^2 = -1$. Es multipliquen seguint les regles que il·lustra la Figura 1.

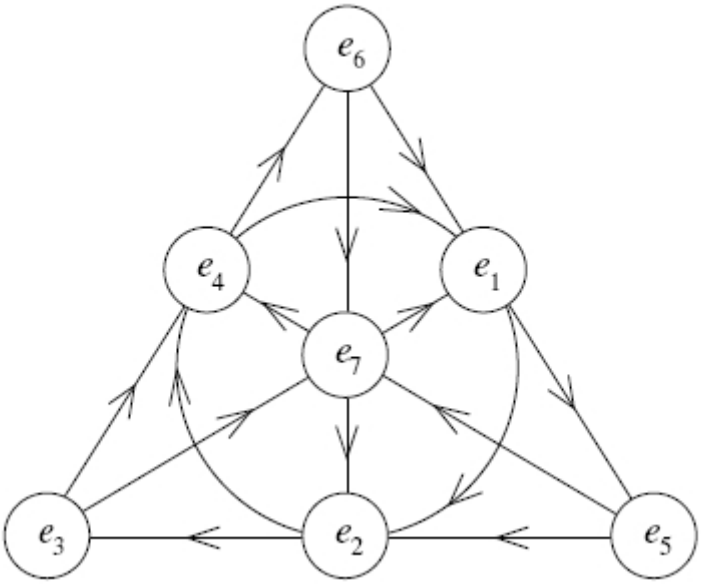

Figura 1: Cada parella d'octonions està sobre una única linia i en aquesta hi ha un tercer octonió, que és el resultat de multiplicar els dos primers en l'ordre que estableix el sentit de les fletxes.

3 L'anell dels enters de Hurwitz

En aquesta secció veurem com són els ordres del cos dels quaternions racionals $\mathbb{H}_{\mathbb{Q}}$, i n'estudiarem un en particular, anomenat els enters de Hurwitz. Per saber què són els ordres veurem com són els elements enters de les $\mathbb{Q}$-àlgebres de quaternions, i en particular, del cos $\mathbb{H}_{\mathbb{Q}}$.

3.1 Enters de les àlgebres de quaternions racionals

En general, si tenim una àlgebra A sobre $\mathbb{Q}$ (no necessàriament no commutativa), diem que $x \in A$ és enter sobre $\mathbb{Z}$ si $\mathbb{Z}[x]$ és un $\mathbb{Z}$-mòdul finitament generat. En el cas de les àlgebres commutatives, la definició d'element enter correspon amb la que utilitzem normalment. Ho veurem amb el resultat següent.

Proposició 3.1. *Sigui A una $\mathbb{Q}$-àlgebra commutativa. És equivalent:*

i) $x \in A$ és un enter sobre $\mathbb{Z}$.

ii) x és arrel d'un polinomi mònic de coeficients en $\mathbb{Z}$, és a dir, existeixen $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ tals que

$$x^n + a^{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Demostració. i) $\Rightarrow$ ii)

Sigui $M = \mathbb{Z}[x]$ un $\mathbb{Z}$-mòdul finitament generat, i siguin $x_1, x_2, \ldots, x_n$ els generadors de M. Tenim que

$$xx_i \in \mathbb{Z}[x], \text{ per a tot } 1 \leq i \leq n,$$

i, per tant, existeixen a_{ij} tals que

$$xx_i = \sum_j a_{ij}x_j \text{ per a tot } 1 \leq i \leq n \ .$$

Per tant, tenim n identitats que es poden escriure en forma de matriu de la manera següent.

$$\begin{pmatrix} a_{11}-x & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22}-x & a_{23} & \cdots & a_{2n} \\ \vdots & \ddots & & & \\ a_{1n} & \cdots & & \cdots & a_{nn}-x \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Si anomenem B la matriu del sistema, tenim que $\det B = 0$. Com que $\det B$ és un polinomi mònic en x de coeficients formats per sumes i productes de $a_{ij} \in \mathbb{Z}$, ja estem.

ii) $\Rightarrow$ i)

Tenim que $x^n + a^{n-1}x^{n-1} + \cdots + a_0 = 0$ amb $a_i \in \mathbb{Z}$. Utilitzant aquesta relació, podem escriure x^n com

$$x^n = -a^{n-1}x^{n-1} - \cdots - a_0$$

i, per tant, $1, x, x^2, \cdots, x^{n-1}$ generen $\mathbb{Z}[x]$.

□

Aquesta caracterització dels enters no es pot estendre en les àlgebres no commutatives perquè en la demostració hem utilitzat aquesta propietat. A partir d'ara, per parlar d'elements enters a les àlgebres de quaternions utilitzarem la següent proposició.

Proposició 3.2. *Sigui H una $\mathbb{Q}$-àlgebra de quaternions, un element $\alpha \in H$ és enter si i només si*

$$N(x) = x\bar{x} \in \mathbb{Z} \text{i} Tr(x) = x + \bar{x} \in \mathbb{Z}.$$

Demostració. $\Leftarrow$

Suposem que $N(\alpha) \in \mathbb{Z}$, i $Tr(\alpha) \in \mathbb{Z}$. Construïm un polinomi que anul·li α.

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha}.$$

Aleshores, tenim que $\alpha^2 - Tr(\alpha)\alpha + N(\alpha) = 0$. Per tant, podem escriure α^2 com $\alpha^2 = Tr(\alpha)\alpha + N(\alpha)$. Qualsevol element del $\mathbb{Z}$-mòdul $\mathbb{Z}[\alpha]$ es pot escriure com a combinació en $\mathbb{Z}$ de 1 i α. Aleshores, $\mathbb{Z}[\alpha]$ és finitament generat.

$\Rightarrow$

Sigui $\alpha \notin \mathbb{Z}$ tal que $\mathbb{Z}[\alpha]$ és finitament generat. Com que $\alpha \notin \mathbb{Z}$ es té que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Aleshores, existeix un polinomi amb coeficients a, b, c en $\mathbb{Q}$ tal que:

$$a\alpha^2 + b\alpha + c = 0.$$

D'altra banda, com que $\mathbb{Z}[\alpha]$ és finitament generat, $\mathbb{Z}[\alpha] = \langle 1, \alpha \rangle$ i $\alpha^2 = b'\alpha + c'$. El polinomi

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha}$$

té arrels α i $\bar{\alpha}$, per tant $Tr(\alpha) = b \in \mathbb{Z}$ i $N(\alpha) = -c \in \mathbb{Z}$. □

Observem que els elements enters de H no formen un anell, vegem-ho amb un exemple en el cas de l'àlgebra $\mathbb{H}_{\mathbb{Q}}$. Siguin

$$\alpha = 1 + i + j + k$$
$$\beta = 1 + \frac{5}{13}i + \frac{11}{13}j + \frac{19}{13}k$$

enters de $\mathbb{H}_{\mathbb{Q}}$ ja que $N(\alpha) = 4$, $N(\beta) = 4$, $Tr(\alpha) = 1$ i $Tr(\beta) = 2$. Aleshores la suma de α i β no és entera ja que

$$\alpha + \beta = 2 + \frac{18}{13}i + \frac{24}{13}j + \frac{32}{13}k$$

i $N(\alpha + \beta) = \frac{200}{13} \notin \mathbb{Z}$.

Definició 3.1. Diem que un anell $\mathcal{O}$ és un *ordre* de H si està format per elements enters de H, conté a $\mathbb{Z}$ i $\mathbb{Q}\mathcal{O} = H$.

3.2 L'anell $\mathcal{O}_H$ dels enters de Hurwitz

Hurwitz no defineix els enters del cos de quaternions $\mathbb{H}_\mathbb{Q}$ tal com nosaltres els coneixem. Per això, anomenarem enters de Hurwitz els enters que presenta Hurwitz en l'article original, i després observarem que aquests són un ordre maximal de $\mathbb{H}_\mathbb{Q}$. Hurwitz busca un $\mathbb{Z}$-mòdul finitament generat que contingui les unitats $\{1, i, j, k\}$, i que, a més, el producte dels seus elements sigui intern.

Teorema 3.1. *Un $\mathbb{Z}$-mòdul J finitament generat a $\mathbb{H}_\mathbb{Q}$, tal que el producte dels seus elements és intern i conté les unitats $\{1, i, j, k\}$, és*

$$J = \mathbb{Z}[i, j, k, \frac{1+i+j+k}{2}], \text{ o bé } J = \mathbb{Z}[1, i, j, k].$$

Demostració. Sigui J el $\mathbb{Z}$-mòdul finitament generat amb les propietats de l'enunciat. Considerem un sistema de generadors $q_1, q_2, \ldots, q_r \in \mathbb{H}_\mathbb{Q}$. Aleshores, tot $q \in J$ es pot escriure com

$$q = m_1 q_1 + m_2 q_2 + \ldots + m_r q_r$$

amb m_i de $\mathbb{Z}$. D'altra banda, q també el podem escriure com

$$q = \frac{a + bi + cj + dk}{m}$$

amb $a, b, c, d, m \in \mathbb{Z}$, posant m el *mcd* dels denominadors de les components de q_i.

Primer de tot veurem que aquest sistema de generadors pot ser reduït a quatre generadors. Fixat el m, seleccionem un $q \in J, q = \frac{1 + bi + cj + dk}{m}$ de manera que el coeficient d és el més petit possible (en valor absolut). Definim

$$q_4 = \frac{d_1 + d_2 i + d_3 j + d_4 k}{m}$$

amb $d_i \in \mathbb{Z}$ i d_4 tal que $d - k_4 d_4 = 0$ per algun $k_4 \in \mathbb{Z}$. Si $d = 0$ prenem $q_4 = 0$. Altrament, tenim que

$$q - k_4 q_4 = \frac{a' + b'i + c'j}{m}.$$

Ara definim

$$q_3 = \frac{c_1 + c_2 i + c_3 j}{m}$$

amb $c_i \in \mathbb{Z}$ i c_3 tal que $c' - k_3 c_3 = 0$. Si $c' = 0$, prenem $q_3 = 0$. Altrament, obtenim que

$$q - k_4 q_4 - k_3 q_3 = \frac{a'' + b''i}{m}.$$

Repetint el procés, obtenim $q_2 = \frac{b_1 + b_2 i}{m}$ i $k_2 \in \mathbb{Z}$ tals que

$$q - (k_4 q_4 + k_3 q_3 + k_2 q_2) = \frac{a'''}{m}.$$

Finalment, posant $q_1 = \dfrac{a_1}{m}$ i $k_1 \in \mathbb{Z}$ tenim que q es posa en combinació de q_1, q_2, q_3, q_4 de la forma següent:

$$q = k_1 q_1 + k_2 q_2 + k_3 q_3 + k_4 q_4.$$

Observem que, al haver agafat el mínim coeficient d de tots els elements de J, tots els quaternions amb la d més gran es podran escriure com a combinació dels q_1, q_2, q_3, q_4. Hem vist que el sistema de generadors de J es pot reduir als quatre elements següents.

$$q_1 = a_1, \quad q_2 = b_1 + b_2 i, \quad q_3 = c_1 + c_2 i + c_3 j, \quad q_4 = d_1 + d_2 i + d_3 j + d_4 k$$

amb $a_i, b_i, c_i, d_i \in \mathbb{Q}$.

Fins ara, només hem utilitzat que J és un $\mathbb{Z}$-mòdul finitament generat. A continuació, determinarem qui són els generadors q_i. La primera observació que hem de fer és que si les unitats $1, i, j, k$ són de J, els elements a_1, b_2, c_3, d_4 han de ser ≤ 1.

El producte en J és intern, i en particular, $q_i^2 \in J$.

$$q_1^2 \in J \Rightarrow q_1^2 = k_1 q_1 \Rightarrow q = k_1 \in \mathbb{Z} \Rightarrow q_1 = 1 \tag{3.1}$$

$$q_2^2 \in J \Rightarrow q_2^2 = (b_1 + b_2 i)^2 = 2b_1(b_1 + b_2 i) - (b_1^2 + b_2^2) = 2b_1 q_2 - (b_1^2 + b_2^2).$$

D'altra banda, $q_2^2 = k_1 q_1 + k_2 q_2 = k_1 + k_2 q_2$.

$$\left.\begin{array}{l} q_2^2 = 2b_1 q_2 - (b_1^2 + b_2^2) \\ q_2^2 = k_2 q_2 + k_1 \end{array}\right. \quad \Longrightarrow \quad k_1 = -(b_1^2 + b_2^2) \Rightarrow (2b_1)^2 + (2b_2)^2 = -4k_1 \Rightarrow$$

$$(2b_1)^2 + (2b_2)^2 \equiv 0 \pmod 4 \Rightarrow b_1, b_2 \in \mathbb{Z}.$$

Com que $b_2 \leq 1$ i $b_2 \in \mathbb{Z}$, es té que $b_2 = 1$ i per tant, $q_2 = b_1 + i$. Fent el canvi $q_2 - b_1 q_1$, posarem que

$$q_2 = i. \tag{3.2}$$

Fem el mateix per q_3.

$$q_3^2 \in J \Rightarrow q_3^2 = (c_1 + b_2 i + c_3 k)^2 = 2c_1(c_1 + b_2 i + c_3 k) - (c_1^2 + c_2^2 + c_3^2) = 2c_1 q_3 - (c_1^2 + c_2^2 + c_3^2).$$

També tenim que $q_3^2 = k_1 + k_2 i + k_3 q_3$. Podem posar que $k_2 = 0$ perquè a l'equació anterior no apareixen termes multiplicats per i.

$$\left.\begin{array}{l} q_3^2 = 2c_1 q_3 - (c_1^2 + c_2^2 + c_3^2) \\ q_3^2 = k_3 q_3 + k_1 \end{array}\right. \Rightarrow k_1 = -(c_1^2 + c_2^2 + c_3^2) \Rightarrow (2c_1)^2 + (2c_2)^2 + (2c_3)^2 = -4k_1$$

$$\Rightarrow (2c_1)^2 + (2c_2)^2 + (2c_3)^2 \equiv 0 \pmod 4 \Rightarrow c_1, c_2, c_3 \in \mathbb{Z}.$$

Com que $c_3 \leq 1$ i $c_3 \in \mathbb{Z}$, es té que $c_3 = 1$ i per tant, $q_2 = c_1 + c_2 i + j$. Si fem $q_3 - c_2 q_2 - c_1 q_1 = q_3 - c_2 i - c_1 = c_3 j = j$. Podem intercanviar q_3 per

$$q_3 = j. \tag{3.3}$$

Per q_4 no podem utilitzar el mateix argument perquè quan féssim la congruència de $(2d_1)^2+(2d_2)^2+(2d_3)^2+(2d_4)^2 \equiv 0 \pmod 4$ no podríem concloure que $d_i \in \mathbb{Z}$. Utilitzem la identitat següent.

$$-iq_4i + q_4 = 2d_1 + 2d_2i$$

Com que $-iq_4i \in J$, i l'hem pogut escriure com a combinació dels generadors $q_1 = 1$ i $q_2 = i$, es té que $2d_1, 2d_2 \in \mathbb{Z}$. Repetint aquest argument conjugant per j obtenim que

$$-jq_4j + q_4 = 2d_1 + 2d_3j \Longrightarrow 2d_3 \in \mathbb{Z}$$

Recordem que $q_4 = d_1+d_2i+d_3j+d_4k$, aleshores $2q_4-2d_1-2d_2i-2d_3j = 2d_4k \in J$. Per tant, $2d_4kk = -2d_4 \in J \Rightarrow 2d_4 \in \mathbb{Z}$. Amb la condició de que $d_4 \leq 1$, obtenim que o bé $d_4 = 1$ o bé $d_4 = \frac{1}{2}$.

Amb el que hem vist fins ara, tenim que qualsevol element de J es pot escriure com

$$q = r + si + tj + uk, \text{ amb } 2r, 2s, 2t \in \mathbb{Z}.$$

Per tant, podem agafar d_1, d_2 i d_3 o bé 0 o bé $\dfrac{1}{2}$. Finalment,

$$q_4^2 = 2d_1q_4 - (d_1^2 + d_2^2 + d_3^2 + d_4^2) \Longrightarrow (d_1^2 + d_2^2 + d_3^2 + d_4^2) \in \mathbb{Z}$$

$$\Longrightarrow (2d_1)^2 + (2d_2)^2 + (2d_3)^2 + (2d_4)^2 \equiv 0 \pmod 4.$$

Si $d_4 = 1$, es té l'equació $(2d_1)^2 + (2d_2)^2 + (2d_3)^2 \equiv 0 \pmod 4$ i si $d_i \in \{0, \frac{1}{2}\}$, la única solució de l'equació és $d_1 = d_2 = d_3 = 0$.

Si $d_4 = \frac{1}{2}$, es té l'equació $(2d_1)^2 + (2d_2)^2 + (2d_3)^2 + 1 \equiv 0 \pmod 4$ i, per tant, $d_1 = d_2 = d_3 = \frac{1}{2}$. Aleshores posarem q_4 com

$$\begin{aligned} &q_4 = k, \\ &\text{o bé,} \\ &q_4 = \frac{1+i+j+k}{2}. \end{aligned} \tag{3.4}$$

Finalment, hem trobat que els generadors de J han de ser els que mostren les equacions 3.1, 3.2, 3.3 i 3.4 i, per tant, els dos possibles $\mathbb{Z}$-mòduls que satisfan les condicions de l'enunciat del teorema són

$$\mathbb{Z}[1, i, j, \frac{1+i+j+k}{2}] \quad \text{i} \quad \mathbb{Z}[1, i, j, k].$$

□

D'ara en endavant, posarem que $\rho = \frac{1+i+j+k}{2}$ i, amb aquesta notació escriurem el $\mathbb{Z}$-mòdul $\mathbb{Z}[1, i, j, \frac{1+i+j+k}{2}]$ com

$$\mathbb{Z}[\rho, i, j, k].$$

Observem que $\mathbb{Z}[1, i, j, k]$ és un submòdul de $\mathbb{Z}[\rho, i, j, k]$. En efecte, sigui $g = a + bi + cj + dk$, amb $a, b, c, d \in \mathbb{Z}$. Aleshores, $g = 2a\rho + (b-a)i + (c-a)j + (d-a)k \in \mathbb{Z}[\rho, i, j, k]$.

Observació 3. $\mathbb{Z}[\rho, i, j, k]$ és un anell d'enters del cos $\mathbb{H}_{\mathbb{Q}}$.

Per una banda, observem que el producte dels elements de $\mathbb{Z}[\rho, i, j, k]$ és intern, i conté la unitat del producte, per tant $\mathbb{Z}[\rho, i, j, k]$ és un anell. D'altra banda, si

$$q = k_0\rho + k_1 i + k_2 j + k_3 k,$$

amb $k_i \in \mathbb{Z}$, aleshores,

$$N(q) = q\bar{q} = k_0^2 + k_1^2 + k_2^2 + k_3^2 + k_0(k_1 + k_2 + k_3) \in \mathbb{Z}$$

i

$$Tr(q) = k_0 \in \mathbb{Z}.$$

Per tant, podem concloure que q és un enter de $\mathbb{H}_{\mathbb{Q}}$, ja que satisfà les condicions de la proposició 3.2.

Definició 3.2. Anomenem anell dels *enters de Hurwitz* l'anell

$$\mathcal{O}_H := \mathbb{Z}[\rho, i, j, k],$$

i designem amb el nom d'enters de Hurwitz els seus elements.

Per una qüestió de facilitat a l'hora de calcular normes, a vegades escriurem els enters de Hurwitz amb la base dels quaternions racionals, $\{1, i, j, k\}$, però imposant algunes condicions sobre els coeficients de q. És a dir, un enter de Hurwitz q es pot posar

$$q = \frac{1}{2}(a + bi + cj + dk)$$

amb $a, b, c, d \in \mathbb{Z}$ complint que o bé són tots parells, o bé són tots senars. Amb aquesta notació, la norma de q és

$$N(q) = \frac{1}{4}(a^2 + b^2 + c^2 + d^2).$$

Observació 4. El centre de $\mathcal{O}_H$ és el cos $\mathbb{Z}$. En efecte, el centre de $\mathcal{O}_H$ conté els racionals, ja que aquests són el centre del cos $\mathbb{H}_{\mathbb{Q}}$. D'altra banda, un element del centre de $\mathcal{O}_H$ commuta amb $1, i, j, k$, per tant ho fa amb tot element de $\mathbb{H}_{\mathbb{Q}}$. Aleshores,

$$Z(\mathcal{O}_H) \subseteq Z(\mathbb{H}_{\mathbb{Q}}) = \mathbb{Q} \Longrightarrow Z(\mathcal{O}_H) = \mathbb{Z}.$$

3.3 El grup de les unitats $\mathcal{O}_H^*$

Definició 3.3. Diem que un enter de Hurwitz ε, és a dir un element $\varepsilon \in \mathcal{O}_H$, és una *unitat* de $\mathcal{O}_H$ si, per a tot $\alpha \in \mathcal{O}_H$, existeix un $u \in \mathcal{O}_H$ tal que

$$\alpha = u\varepsilon.$$

En aquest cas, posem que $\varepsilon \in \mathcal{O}_H^*$.

Amb la noció de divisibilitat que veurem a la secció següent, aquesta definició es pot pensar com

$$\varepsilon \in \mathcal{O}_H^* \iff \varepsilon \text{ divideix a } \alpha \text{ per la dreta, per a tot } \alpha \in \mathcal{O}_H.$$

Observem que, en particular, si ε és una unitat, aleshores existeix un $u \in \mathcal{O}_H$ tal que

$$1 = u\varepsilon \Rightarrow 1 = N(u)N(\varepsilon) \Rightarrow N(\varepsilon) = 1$$

Sigui ε^{-1} l'element invers de ε del cos $\mathbb{H}_{\mathbb{Q}}$, recordem que

$$\varepsilon^{-1} = \frac{\bar{\varepsilon}}{N(\varepsilon)} = \bar{\varepsilon} \in \mathcal{O}_H.$$

En conseqüència, obtenim que

$$1 = \varepsilon^{-1}\varepsilon = \varepsilon\varepsilon^{-1} \quad \text{amb } \varepsilon \text{ i } \varepsilon^{-1} \in \mathcal{O}_H.$$

I, per tant, sigui $\alpha \in \mathcal{O}_H$ un enter qualsevol

$$\alpha = \varepsilon\varepsilon^{-1}\alpha.$$

Això, en termes de divisibilitat, es tradueix en què ε divideix per l'esquerra tot enter de Hurwitz α.

Observació 5. $\mathcal{O}_H^*$ és un grup multiplicatiu. En efecte, siguin $\varepsilon, \delta \in \mathcal{O}_H^*$ aleshores $\varepsilon\delta \in \mathcal{O}_H^*$ ja que per a tot $\alpha \in \mathcal{O}_H$,

$$\alpha = \alpha\varepsilon^{-1}\varepsilon,$$
$$\alpha = \alpha\delta^{-1}\delta.$$

Fixat un α, considerem $\beta = \alpha\delta^{-1}$. Aleshores,

$$\beta = \beta\varepsilon^{-1}\varepsilon \Rightarrow \alpha = \alpha(\delta^{-1}\varepsilon^{-1})\varepsilon\delta, \quad \text{ i } \alpha\delta^{-1}\varepsilon^{-1} \in \mathcal{O}_H.$$

Per tant, $\varepsilon\delta$ és una unitat de $\mathcal{O}_H$ i $\varepsilon\delta \in \mathcal{O}_H^*$.

Recordem algunes nocions del subgrup del grup simètric S_4 de les permutacions parelles, el que coneixem com el grup alternat A_4. Aquest grup està format per les permutacions parelles del tetraedre, i per tant, els seus elements són de la forma $(ij)(kl)$ amb $i, j, k, l \in \{1, 2, 3, 4\}$ tals que $i \neq j$ i $k \neq l$. A més, el grup alternat A_4 té dues extensions centrals de nucli C_2. Una és el producte cartesià $C_2 \times A_4$ i l'altra és un producte semidirecte $2A_4$. Aquest grup s'anomena el grup binari tetraèdric, atès que A_4 és isomorf al grup de les rotacions de l'espai que preserven un tetràedre regular. Aquest grup es pot obtenir a partir de les successions exactes (veure proposició 7.2)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_2 & \longrightarrow & \mathrm{Spin}_3(\mathbb{R}) & \longrightarrow & SO_3(\mathbb{R}) & \longrightarrow & 1 \\ & & & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & C_2 & \longrightarrow & A_4 & \longrightarrow & A_4 & \longrightarrow & 1 \end{array} \tag{3.5}$$

Teorema 3.2 (d'estructura de $\mathcal{O}_H^*$)**.** *Sigui $\mathcal{O}_H^*$ el grup multiplicatiu de les unitats de $\mathcal{O}_H$. Aleshores:*

1. $\mathcal{O}_H^* = \{\pm 1, \pm i, \pm j, \pm k, \dfrac{\pm 1 \pm i \pm j \pm k}{2}\}$.
2. *El grup $\mathcal{O}_H^*$ està generat pels elements $\{\pm v_1, \pm v_2, \pm g\}$, on*

$$\begin{aligned} v_1 &= -i, \\ v_2 &= -j, \\ g &= \frac{1-i-j-k}{2}. \end{aligned}$$

3. *$\mathcal{O}_H^*$ és isomorf al grup binari tetraèdric $\widetilde{A}_4 = 2A_4$.*

Demostració. 1. Si posem $\varepsilon \in \mathcal{O}_H^*$ en la base de $\mathbb{H}_{\mathbb{Q}}$, $\varepsilon = \frac{1}{2}(a + bi + cj + dk)$ amb a, b, c, d nombres enters tals que són o bé tots parells o bé tots senars. La condició que $N(\varepsilon) = 1$ es tradueix en l'equació

$$\frac{1}{4}(a^2 + b^2 + c^2 + d^2) = 1.$$

- Si a, b, c, d són enters senars, aleshores tenim que $a^2, b^2, c^2, d^2 \geq 1$ i, per tant,
$$\frac{1}{4}(a^2 + b^2 + c^2 + d^2) = 1 \Longleftrightarrow a, b, c, d = \pm 1.$$
D'aquí obtenim les 16 unitats $\varepsilon = \dfrac{\pm 1 \pm i \pm j \pm k}{2}$.
- Si a, b, c, d són parells, suposem que n'hi ha almenys dos diferents de zero, per exemple a, b. Tenim que
$$\frac{1}{4}(a^2 + b^2 + c^2 + d^2) \geq \frac{1}{4}(a^2 + b^2) \geq \frac{1}{4}(8) = 2 > 1.$$
Per tant, sol pot donar-se el cas en que un únic coeficient és diferent de zero. Suposem que $a \neq 0$, $\frac{1}{4}(a^2) = 1 \Leftrightarrow a = \pm 2$. Fent el mateix amb b, c i d obtenim les unitats $\varepsilon = \pm 1, \pm i, \pm j, \pm k$.

2. Amb un càlcul es pot veure que $\mathcal{O}_H^*/C_2$ és el grup generat per les classes d'equivalència (respecte el canvi de signe) dels elements:

$$\begin{aligned} v_1 &= \frac{1}{2}(e_1 - e_3)(e_2 - e_4) = -i, \\ v_2 &= \frac{1}{2}(e_1 - e_4)(e_2 - e_3) = -j, \\ g &= \frac{1}{2}(e_1 - e_2)(e_2 - e_3) = \frac{1-i-j-k}{2}. \end{aligned}$$

En efecte,

$$\begin{aligned}&\{1, v_1, v_2, v_1v_2, g, gv_1, gv_2, gv_1v_2, g^2, g^2v_1, g^2v_2, g^2v_1v_2\}\\ =&\{1, -i, -j, k, \frac{1-i-j-k}{2}, \frac{-1-i+j-k}{2}, \frac{-1-i-j+k}{2}, \frac{1-i+j+k}{2},\\ &\frac{-1-i-j-k}{2}, \frac{-1+i+j-k}{2}, \frac{-1-i+j+k}{2}, \frac{1-i+j-k}{2}\}\end{aligned}$$

Per tant, $\mathcal{O}_H^*$ està generat per $\pm v_1, \pm v_2$ i $\pm g$.

3. Anteriorment hem dit que les dues extensions centrals de nucli C_2 del grup alternat A_4 són $A_4 \times C_2$ i el grup binari tetraèdric $\widetilde{A_4}$. Està clar que $\mathcal{O}_H^*$ no és isomorf a $A_4 \times C_2$. Per tant, si trobem un isomorfisme entre $\mathcal{O}_H^*/C_2$ i A_4, podrem concloure que $\mathcal{O}_H^* \cong \widetilde{A_4}$.

   Considerem el morfisme

$$\begin{aligned}\Phi : \mathrm{Spin}_3(\mathbb{R}) &\longrightarrow SO_3(\mathbb{R})\\ u &\longmapsto \varphi_u(r) = uru^{-1}.\end{aligned}$$

   definit a la secció 2 a la proposició 7.2. Recordem que $\mathrm{Spin}_3(\mathbb{R})$ és el conjunt

$$\mathrm{Spin}_3(\mathbb{R}) = \{q \in \mathbb{H} \mid N(q) = 1\}.$$

   Per tant, $\mathcal{O}_H^*$ està contingut en $\mathrm{Spin}_3(\mathbb{R})$ i podem restringir Φ al grup de les unitats $\mathcal{O}_H^*$, obtenint així el morfisme:

$$\begin{aligned}\Phi_{|\mathcal{O}_H^*} : \mathcal{O}_H^* &\longrightarrow SO_3(\mathbb{R})\\ \varepsilon &\longmapsto \varphi_\varepsilon(r) = \varepsilon r\varepsilon^{-1}.\end{aligned}$$

   Considerem el tetràedre regular de $\mathbb{R}^3$ format pels vèrtexs

$$P_1 = (-1, 1, -1), \quad P_2 = (1, -1, -1), \quad P_3 = (-1, -1, 1), \quad P_4 = (1, 1, 1).$$

   Pensant $\mathbb{R}^3$ com l'espai dels quaternions purs, anomenem $p_i \in \mathbb{H}$ els quaternions situats en els punts P_i, és a dir,

$$p_1 = -i + j - k, \quad p_2 = i - j - k, \quad p_3 = -i - j + k, \quad p_4 = i + j + k.$$

   Anem a veure que les rotacions $\varphi_\varepsilon(r)$ que defineixen els elements v_1, v_2 i g, són permutacions dels vèrtex del tetràedre representats segons (p_1, p_2, p_3, p_4).

   - $v_1 = -i$: $\varphi_{v_1}(r) = -ir(-i)^{-1} = -iri$. Aleshores:

$$\begin{aligned}\varphi_{v_1}(p_1) &= \varphi_{v_1}(-i + j - k) = -i - j + k = p_3,\\ \varphi_{v_1}(p_2) &= \varphi_{v_1}(i - j - k) = i + j + k = p_4,\\ \varphi_{v_1}(p_3) &= \varphi_{v_1}(-i - j + k) = -i + j - k = p_1,\\ \varphi_{v_1}(p_4) &= \varphi_{v_1}(i + j + k) = i - j - k = p_2,\end{aligned}$$

     Per tant, numerant els vèrtex del tetràedre obtenim que φ_{v_1} és la permutació $\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix} = (13)(24)$.

- $v_2 = -j$: $\varphi_{v_2}(r) = -jr(-j)^{-1} = -jrj$. Aleshores, fent els càlculs corresponents es pot veure que la permutació del tetràedre que defineix φ_{v_2} és
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23).$$
- $g = \dfrac{1-i-j-k}{2}$: $\varphi_g(r) = grg^{-1} = \dfrac{1-i-j-k}{2} r \dfrac{1+i+j+k}{2}$. Aleshores, fent els càlculs corresponents es pot veure que la permutació del tetràedre que defineix φ_g és
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (12)(23).$$

Utilitzant tot el que acabem de veure, podem definir el morfisme

$$\begin{aligned} \varphi : \mathcal{O}_H^* &\longrightarrow A_4 \\ \varepsilon &\longmapsto \varphi(\varepsilon) \end{aligned} \tag{3.6}$$

on $\varphi(\varepsilon)$ és la permutació dels vèrtexs del tetràedre que defineix la rotació φ_ε. Atès que $\varphi_{v_1}, \varphi_{v_1}$ i φ_g són permutacions del tetràedre, i per a tot $\varepsilon \in \mathcal{O}_H^*$, ε és producte de $\pm v_1, \pm v_2$ i $\pm g$, aleshores la rotació φ_ε és una permutació dels vèrtexs del tetràedre.

Amb un càlcul, s'obté que el grup alternat A_4 està generat per les permutacions $\sigma_1 = (13)(24), \sigma_2 = (14)(23), \tau = (12)(23)$. En efecte,

$$\begin{aligned} &\{Id, \sigma_1, \sigma_2, \sigma_1\sigma_2, \tau, \tau\sigma_1, \tau\sigma_2, \tau\sigma_1\sigma_2, \tau^2, \tau^2\sigma_1, \tau^2\sigma_2, \tau^2\sigma_1\sigma_2\} \\ =&\{Id, (13)(24), (14)(23), (12)(34), (123), (243), \\ &(142), (134), (132), (124), (143), (234)\} \end{aligned}$$

i, per tant, tota permutació de A_4 es pot obtenir mitjançant composicions de σ_1, σ_2 i τ. Això ens diu que tota permutació del tetràedre es pot obtenir a partir de una composició adequada de les rotacions $\varphi_{v_1}, \varphi_{v_2}$ i φ_g. Per tant, el morfisme $\varphi : \mathcal{O}_H^* \longrightarrow A_4$ és exhaustiu.

Finalment, calculem el $\mathrm{Ker}(\varphi)$.

$$\varphi(\varepsilon) = Id \iff \varphi_\varepsilon(r) = \varepsilon r \varepsilon^{-1} = r \text{ per a tot } r \in \mathbb{H} \iff \varepsilon = \pm 1.$$

Així, $\mathrm{Ker}(\varphi) \cong C_2$. Pel teorema d'isomorfia tenim que

$$\mathcal{O}_H^* / C_2 \cong A_4.$$

I finalment obtenim que

$$\mathcal{O}_H^* \cong \widetilde{A_4}.$$

□

3.4 Automorfismes de $\mathcal{O}_H$

En la primera secció hem pogut veure que tots els automorfismes del cos $\mathbb{H}_\mathbb{Q}$ són interns, és a dir, que tot automordisme del cos dels quaternions racionals es pot posar com qrq^{-1} per un cert $q \in \mathbb{H}_\mathbb{Q}$. L'objectiu d'aquesta secció és trobar els automorfismes que deixen invariant l'anell dels enters de Hurwitz. Anomenarem aquests automorfismes, automorfismes de $\mathcal{O}_H$.

Podem observar que els automorfismes definits per les unitats de l'anell $\mathcal{O}_H$, deixen invariant aquest anell. En efecte, siguin $\alpha \in \mathcal{O}_H$, $\varepsilon \in \mathcal{O}_H^*$,

$$f(\alpha) = \varepsilon\alpha\varepsilon^{-1} \in \mathcal{O}_H \quad \text{ja que } \mathcal{O}_H \text{ és un anell.} \tag{3.7}$$

Tot i així, els automorfismes que estem buscant no són únicament els que vénen definits per unitats, ja que si agafem $\zeta = 1 + i$ aleshores

$$f(\alpha) = \zeta\alpha\zeta^{-1} = (1+i)\frac{1}{2}(a + bi + cj + dk)(\frac{1+i}{2}) = \frac{1}{2}(a + bi - dj + ck).$$

que pertany a $\mathcal{O}_H$ perquè si $\alpha = \frac{1}{2}(a + bi + cj + dk) \in \mathcal{O}_H$ aleshores a, b, c, d són o bé tots parells o bé tots senars. Combinant ζ amb una unitat ε obtenim un altre tipus d'automorfisme,

$$f(\alpha) = \varepsilon\zeta\alpha(\varepsilon\zeta)^{-1} = \varepsilon\zeta\alpha\zeta^{-1}\varepsilon^{-1}. \tag{3.8}$$

Teorema 3.3. *1. Tot automorfisme de $\mathcal{O}_H$ està definit per*

$$\begin{aligned} f: \quad & \mathbb{H} \longrightarrow \mathbb{H} \\ & i \longmapsto \pm\alpha, \\ & j \longmapsto \pm\beta, \\ & k \longmapsto \pm\gamma, \end{aligned}$$

on (α, β, γ) és una permutació de (i, j, k) de manera que $\pm\alpha \cdot \pm\beta \cdot \pm\gamma = -1$.

2. $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z}) \cong S_4$.

Demostració. 1. Considerem un automorfisme $f : \mathcal{O}_H \longrightarrow \mathcal{O}_H$. Anomenem α, β i γ les imatges per f de i, j i k respectivament. Aleshores es té que

$$\alpha^2 = \beta^2 = \gamma^2 = -1, \quad \alpha\beta\gamma = -1.$$

En particular, per a α es té que si

$$\alpha = \frac{1}{2}(a + bi + cj + dk) \quad \text{amb } a, b, d \text{ i } d \text{ tots parells o senars}$$

aleshores,

$$\alpha^2 = \frac{a}{2}(a+bi+cj+dk) - \frac{a^2+b^2+c^2+d^2}{4} = -1 \Rightarrow \begin{cases} ab = 0, \quad ac = 0, \quad ad = 0, \\ \frac{a^2-b^2-c^2-d^2}{4} = -1. \end{cases}$$

El cas $a \neq 0$ el podem descartar perquè si $a \neq 0$ aleshores $b = c = d = 0$ i $\dfrac{a^4}{4} = -1$. Com que b, c i d són enters tots parells o tots senars, tenim les possibilitats següents.

$$\begin{aligned} &a = 0, \quad b = \pm 2, \quad c = 0, \quad d = 0 \Rightarrow \alpha = \pm i, \\ &a = 0, \quad b = 0, \quad c = \pm 2, \quad d = 0 \Rightarrow \alpha = \pm j, \\ &a = 0, \quad b = 0, \quad c = 0, \quad d = \pm 2 \Rightarrow \alpha = \pm k. \end{aligned}$$

Aplicant el mateix procediment a β i a γ s'obté que $\alpha, \beta, \gamma \in \{\pm i, \pm j, \pm k\}$. Observem que no pot ser que α i β tinguin la mateixa imatge (o amb un canvi de signe) perquè si fos així tindríem que

$$\gamma = f(k) = f(ij) = f(i)f(j) = (\pm i)(\pm i) = \pm 1 \notin \{\pm i, \pm j, \pm k\}.$$

Per tant, α, β i γ són una permutació de $\{i, j, k\}$ tals que $\alpha\beta\gamma = -1$. Recordem que aquest tipus d'automorfismes els hem estudiat anteriorment, són l'exemple 6 de la secció 2. Ja hem vist que d'aquests automorfismes n'hi ha 24. Per tant, en total, hi ha 24 automorfismes de $\mathcal{O}_H$.

2. Per demostrar l'isomorfisme $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z}) \cong S_4$ anem a veure primer que tots els automorfismes són del tipus 3.7 o del tipus 3.8. Després construirem un isomorfisme entre el conjunt d'aquests dos tipus d'automorfismes, i el grup S_4.

   Part 1: Veurem que hi ha exactament 12 automorfismes diferents del tipus 3.7 i 12 automorfismes diferents del tipus 3.8.

   Siguin $\varepsilon_1, \varepsilon_2 \in \mathcal{O}_H^*$ unitats diferents. Suposem que defineixen el mateix automorfisme, és a dir, per a tot $\alpha \in \mathcal{O}_H$,

   $$\varepsilon_1 \alpha \varepsilon_1^{-1} = \varepsilon_2 \alpha \varepsilon_2^{-1} \Rightarrow \alpha \varepsilon_1^{-1} \varepsilon_2 = \varepsilon_1^{-1} \varepsilon_2 \alpha.$$

   Com que $\varepsilon_1^{-1}\varepsilon_2$ commuta amb qualsevol $\alpha \in \mathcal{O}_H$, $\varepsilon_1^{-1}\varepsilon_2$ ha de ser del centre de $\mathcal{O}_H$, que com hem observat en 4, és $\mathbb{Z}$. Per tant, tenim que $\varepsilon_1^{-1}\varepsilon_2 = r \in \mathbb{Z}$. D'altra banda, $\varepsilon_1^{-1}\varepsilon_2$ és una unitat, ja que $\mathcal{O}_H^*$ és un grup. Aleshores,

   $$1 = N(\varepsilon_1^{-1}\varepsilon_2) = N(r) = r^2 \Rightarrow r = \pm 1 \Rightarrow \begin{cases} \varepsilon_1 = \varepsilon_2, \\ \text{ o bé,} \\ \varepsilon_1 = -\varepsilon_2. \end{cases}$$

   El primer cas no pot ser perquè hem suposat que $\varepsilon_1 \neq \varepsilon_2$. Recordem que el grup de les unitats està format per 24 elements, i si fem classes d'equivalència mòdul el canvi de signe, obtenim

   $$\mathcal{O}_H^* / C_2 \cong A_4,$$

   i el grup A_4 té 12 elements. Aleshores, hi ha 12 automorfismes diferents del tipus 3.7.

   Recordem que els automorfismes del tipus 3.8 són de la forma

   $$f(\alpha) = \varepsilon \zeta \alpha \zeta^{-1} \varepsilon^{-1}$$

per a $\zeta = 1 + i$ i ε una unitat. Pel mateix que acabem de veure, dos automorfismes d'aquest tipus són iguals si i només si les unitats que els defineixen són oposades. Per a cada unitat de les 12 que són diferents respecte el canvi de signe, hi ha un automorfisme. Per tant, hi ha 12 automorfismes diferents del tipus 3.8.

Notem que els automorfismes dels dos tipus són tots diferents. En efecte, anem a suposar que tenim $f_1(\alpha) = \varepsilon_1 \alpha \varepsilon_1^{-1}$ i $f_2(\alpha) = \varepsilon_2 \zeta \alpha \zeta^{-1} \varepsilon_2^{-1}$, tals que $f_1(\alpha) = f_2(\alpha)$ per a tot $\alpha \in \mathcal{O}_H$, aleshores

$$\varepsilon_1 \alpha \varepsilon_1^{-1} = \varepsilon_2 \zeta \alpha \zeta^{-1} \varepsilon_2^{-1} \Rightarrow \alpha \varepsilon_1^{-1} \varepsilon_2 \zeta = \varepsilon_1^{-1} \varepsilon_2 \zeta \alpha.$$

Pel mateix raonament que hem fet abans, $\varepsilon_1^{-1} \varepsilon_2 \zeta = r \in \mathbb{Z}$. Aplicant normes,

$$r^2 = N(r) = N(\varepsilon_1^{-1} \varepsilon_2 \zeta) = 2 \Rightarrow r = \sqrt{2} \notin \mathbb{Z}.$$

El nombre total d'automorfismes de $\mathcal{O}_H$ coincideix amb els que hem construit al primer apartat, per tant, hi ha una bijecció entre $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z})$ i $(\mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i))/C_2$. En particular, obtenim que $G = (\mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i))/C_2$ és un grup.

Part 2: Volem veure que $G/C_2 \cong S_4$. Per fer-ho, definim $S = \{S_1, S_2, S_3, S_4\}$ els 3−Sylows del grup $\mathcal{O}_H^*$. N'hi ha 4 perquè pels teoremes de Sylow o bé n'hi ha un o bé 4, i a més G té 8 elements d'ordre 3. Siguin

$$\begin{aligned} u_1 &= \frac{-1 - i + j + k}{2}, \\ u_2 &= \frac{-1 + i - j + k}{2}, \\ u_3 &= \frac{-1 + i + j - k}{2}, \\ u_4 &= \frac{-1 - i - j - k}{2}, \end{aligned}$$

els quatre elements d'ordre 3 que generen subgrups diferents. Aleshores els 4 3-Sylows de S són:

$$S_1 = \{u_1, u_1^2, 1\}, \quad S_2 = \{u_2, u_2^2, 1\}, \quad S_3 = \{u_3, u_3^2, 1\}, \quad S_4 = \{u_4, u_4^2, 1\}.$$

Definim el morfisme

$$\begin{aligned} \varphi : G \times S &\longrightarrow S \\ (\gamma, S_i) &\longmapsto \gamma S_i \gamma^{-1} = S_j. \end{aligned}$$

que està ben definit ja que

- Si $\gamma \in \mathcal{O}_H^*$ aleshores $\gamma S_i \gamma^{-1}$ és un altre 3-Sylow (pels teoremes de Sylow sabem que són tots conjugats).
- Si $\gamma \in \mathcal{O}_H^*(1+i)$, aleshores $\gamma u_i \gamma^{-1} \in \mathcal{O}_H^*$ ja que

$$N(\gamma u_i \gamma^{-1}) = N(\gamma) N(u_i) N(\gamma^{-1}) = N(\gamma) N(\gamma^{-1}) = 1.$$

I a més $\gamma u_i \gamma^{-1}$ té ordre 3 ja que

$$(\gamma u_i \gamma^{-1})^2 = \gamma u_i^2 \gamma^{-1} \neq 1$$
$$(\gamma u_i \gamma^{-1})^3 = \gamma u_i^3 \gamma^{-1} = 1.$$

Aleshores, $\gamma S_i \gamma^{-1}$ és un 3-Sylow.

Per tant, la conjugació dels grups de Sylow pels elements de G ens dóna altres 3-Sylows. A més, fixat un $\gamma \in G$, φ és injectiu, és a dir, $\varphi(\gamma, S_i) \neq \varphi(\gamma, S_j)$ si $i \neq j$. Això ens permet definir una relació entre l'element $\gamma \in G$ i la permutació que fa la conjugació per γ del conjunt S. Obtindrem així una respresentació de G per permutacions. Definim el morfisme:

$$\begin{aligned} \psi \ : G &\longrightarrow S_4 \\ \gamma &\longmapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ i & j & k & l \end{pmatrix} \end{aligned}$$

amb $i, j, k, l \in \{1, 2, 3, 4\}$ tals que

$$S_i = \varphi(\gamma, S_1), \quad S_j = \varphi(\gamma, S_2), \quad S_k = \varphi(\gamma, S_3), \quad S_l = \varphi(\gamma, S_4).$$

Aquest morfisme ψ està ben definit perquè φ és injectiva i aleshores $\psi(\gamma) \in S_4$. El nucli de ψ està format pels $\gamma \in G$ tals que

$$\begin{aligned} \varphi(\gamma, S_1) = S_1 &\Longrightarrow u_1 = \gamma u_1 \gamma^{-1} \Longrightarrow \gamma u_1 = u_1 \gamma, \\ \varphi(\gamma, S_2) = S_2 &\Longrightarrow u_2 = \gamma u_2 \gamma^{-1} \Longrightarrow \gamma u_2 = u_2 \gamma, \\ \varphi(\gamma, S_3) = S_3 &\Longrightarrow u_3 = \gamma u_3 \gamma^{-1} \Longrightarrow \gamma u_3 = u_3 \gamma, \\ \varphi(\gamma, S_4) = S_4 &\Longrightarrow u_4 = \gamma u_4 \gamma^{-1} \Longrightarrow \gamma u_4 = u_4 \gamma. \end{aligned}$$

Resolent els sistema, s'obte que els únics $\gamma \in G$ que satisfan aquestes quatre equacions són $\gamma = \pm 1$ i, per tant, la representació no és fidel atès que $\mathrm{Ker}(\psi) \cong C_2$. Aleshores, si fem quocient en el grup G, obtenim que el morfisme

$$\overline{\psi} : G/C_2 \longrightarrow S_4$$

és injectiu. A la primera part de la demostració ja hem vist que $\sharp G/C_2 = 24$, i a més $\sharp S_4 = 24$, aleshores es té que $\overline{\psi}$ és exhaustiu i, per tant, un isomorfisme. Finalment, utilitzant la bijecció que hem provat anteriorment entre $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z})$ i $(\mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i))/C_2$, obtenim que,

$$\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z}) \cong S_4.$$

□

Demostració alternativa de l'isomorfisme $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z}) \cong S_4$. A la primera part del teorema anterior hem vist que $\sharp\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z}) = 24$, per tant, pels teoremes de Sylow, $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z})$ ha de tenir algun 3-Sylow. D'altra banda, fent servir que els automorfismes són de la forma $f(r) = qrq^{-1}$ per un cert $q \in \mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i)$, veiem

que aquest grup té 8 elements d'ordre 3. Aleshores, $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z})$ té 4 3-Sylows. Si busquem tots els grups finits d'ordre 24 amb 4 3-Sylows, obtenim els grups següents:

$$\widetilde{A_4}, \quad A_4 \times C_2, \quad S_4.$$

Observem ara que el centre dels dos primers grups, $\widetilde{A_4}$ i $A_4 \times C_2$ conté un element d'ordre 2. Però el centre de $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z})$ és la identitat. Vegem-ho:

Sigui $f_q(r) = qrq^{-1}$ un automorfisme de $\mathcal{O}_H$ que commuta amb tot automorfisme de $\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z})$. Aleshores:

$$f_q f_p(r) = f_p f_q(r) \text{ per a tot } p \in \mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i).$$

Fixat un $p \in \mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i)$, es té que

$$\begin{aligned} &qprp^{-1}q^{-1} = pqrq^{-1}p^{-1} \text{ per a tot } r \in \mathcal{O}_H \Longrightarrow rp^{-1}q^{-1}pq = p^{-1}q^{-1}pqr \\ &\Longrightarrow p^{-1}q^{-1}pq \in Z(\mathcal{O}_H) = \mathbb{Z} \Longrightarrow p^{-1}q^{-1}pq = 1 \Longrightarrow q^{-1}pq = p \Longrightarrow q = \pm 1. \end{aligned}$$

Per tant $f_q(r)$ és la identitat. Finalment, com que hem descartat que el grup és isomorf a $\widetilde{A_4}$ i a $A_4 \times C_2$, l'única opció restant és que

$$\mathrm{Aut}(\mathcal{O}_H \mid \mathbb{Z}) \cong S_4.$$

□

4 Divisibilitat a l'anell dels enters de Hurwitz

La noció de divisibilitat a un anell no commutatiu s'ha de diferenciar segons per quin costat s'opera. Així, en aquesta secció veurem què vol dir ser divisible per la dreta o per l'esquerra (o ambdós) per un enter de Hurwitz. A més també parlarem de la divisió entera tal i com la coneixem a l'anell dels nombres enters, i veurem algunes propietats que té $\mathcal{O}_H$ gràcies a tenir un algoritme de divisió entera.

Primer de tot, ens centrarem a respondre la pregunta següent:

Quins són els enters de Hurwitz $v \in \mathcal{O}_H$ tals que si $\alpha \in \mathcal{O}_H$,

$$v \text{ divideix a } \alpha \text{ per l'esquerra} \Longrightarrow v \text{ també divideix a } \alpha \text{ per la dreta?}$$

Definició 4.1. Siguin α i $\beta \in \mathcal{O}_H$ dos enters de Hurwitz. Direm que α és *divisible per la dreta* (resp. *equerra*) per β si existeix un enter de Hurwitz $q \in \mathcal{O}_H$ tal que

$$\alpha = q\beta \quad \text{(resp. } \alpha = \beta q\text{)}.$$

En les mateixes condicions, també podem posar que β divideix per la dreta (resp. esquerra) a α, o bé que β és un divisor de α per la dreta (resp. esquerra) si existeix $q \in \mathcal{O}_H$ tal que $\alpha = q\beta$ (resp. $\alpha = \beta q$).

Observem que és necessari separar les definicions de divisibilitat per la dreta i per l'esquerra ja que si un enter $\beta \in \mathcal{O}_H$ divideix a $\alpha \in \mathcal{O}$ per la dreta, no té perquè dividir α per l'esquerra. Per exemple,

Exemple 8. El quaternió $\beta = 1 + i + j$ divideix a $\alpha = -2 + 2j + k \in \mathcal{O}_H$ per la dreta, en efecte

$$\alpha = -2 + 2j + k = (i + j + k)(1 + i + j) = (i + j + k)\beta,$$

on $i + j + k$ és un enter de Hurwitz. Però, β no divideix a α per l'esquerra perquè si ho fes,

$$\alpha = \beta q \Longrightarrow q = \beta^{-1}\alpha = \frac{i + 5j - k}{3},$$

i q seria de $\mathcal{O}_H$.

Així, no tots els quaternions racionals satisfan la propietat que ens hem preguntat a l'inici de la secció. Caracteritzem els que sí que ho fan amb la definició següent.

Definició 4.2. Diem que un enter de Hurwitz $q \in \mathcal{O}_H$ és *intercanviable* si

$$\{\alpha q \mid \alpha \in \mathcal{O}_H\} = \{q\beta \mid \beta \in \mathcal{O}_H\}.$$

I, per tant, si q és intercanviable es té que si q divideix per la dreta a $\gamma \in \mathcal{O}_H$ aleshores, $\gamma \in \{\alpha q \mid \alpha \in \mathcal{O}_H\}$ i per la igualtat dels dos conjunts, es té que existeix un $\beta \in \mathcal{O}_H$ tal que

$$\gamma = q\beta \Longrightarrow \ q \text{ divideix a } \gamma \text{ per l'esquerra.}$$

Proposició 4.1. *Els quaternions intercanviables són els elements del grup* $\mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i)$.

Demostració. Considerem $q \in \mathcal{O}_H$ un quaternió intercanviable, aleshores sigui un $\alpha \in \mathcal{O}_H$ qualsevol, existeix un $\beta \in \mathcal{O}H$ de manera que

$$\beta q = q\alpha \Longrightarrow \beta = q\alpha q^{-1}.$$

Definim $f_q(r) = qrq^{-1}$l'automorfisme de $\mathcal{O}_H$ tal que aplicat a α, $f_q(\alpha) = q\alpha q^{-1} = \beta$. Per la demostració del teorema 3.3, podem deduïr que q és de la forma

$$q = \begin{cases} \varepsilon \in \mathcal{O}_H^*, \\ \text{ o bé,} \\ \varepsilon(1+i). \end{cases}$$

i, per tant, $q \in \mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i)$. Recordem que al teorema 3.3 havíem vist que

$$(\mathcal{O}_H^* \cup \mathcal{O}_H^*(1+i))/C_2 \cong S_4.$$

Per tant, els quaternions intercanviables constitueixen un doble recobriment de S_4, que podem designar per $\widetilde{S}_4$. □

4.1 Divisió entera a $\mathcal{O}_H$

A continuació, trobarem un algoritme per fer la divisió entera entre dos enters de Hurwitz.

Proposició 4.2. *Donats* $g \in \mathcal{O}_H$ *i* $m \in \mathbb{Z}$, *existeix un* q *de* $\mathcal{O}_H$ *tal que*

$$N(g - qm) < m^2.$$

Demostració. Siguin $g = k_0\rho + k_1 i + k_2 j + k_3 k \in \mathcal{O}_H$ i $m \in \mathbb{Z}$, considerem un enter de Hurwitz qualsevol

$$q = t_0\rho + t_1 i + t_2 j + t_3 k$$

amb $t_0, t_1, t_2, t_3 \in \mathbb{Z}$. Aleshores, les components de $g - qm$ en la base $\{1, i, j, k\}$ són:

$$\begin{aligned} &\frac{1}{2}(k_0 - mt_0), \\ &\frac{1}{2}(k_0 + 2k_1 - m(t_0 + 2t_1)), \\ &\frac{1}{2}(k_0 + 2k_2 - m(t_0 + 2t_2)), \\ &\frac{1}{2}(k_0 + 2k_3 - m(t_0 + 2t_3)). \end{aligned}$$

Aquestes components no tenen perquè ser totes parelles o totes senars, per tant $g - qm$ no té perquè ser un enter de Hurwitz. Però el que sí podem afirmar és que

existeixen t_0, t_1, t_2, t_3 enters tals que les components de $g - qm$ són, en valor absolut, mes petites que $\frac{1}{4}m, \quad \frac{1}{2}m, \quad \frac{1}{2}m, \quad \frac{1}{2}m$ respectivament. Vegem-ho:

$$\begin{aligned}
\frac{1}{2}|k_0 - mt_0| < \frac{1}{4}m &\iff |t_0 - \frac{k_0}{m}| < \frac{1}{2}, \\
\frac{1}{2}|k_0 + 2k_1 - m(t_0 + 2t_1)| < \frac{1}{2}m &\iff |t_1 - (\frac{k_0}{2m} + \frac{k_1}{m}\frac{t_0}{2})| < 1, \\
\frac{1}{2}|k_0 + 2k_2 - m(t_0 + 2t_2)| < \frac{1}{2}m &\iff |t_2 - (\frac{k_0}{2m} + \frac{k_2}{m}\frac{t_0}{2})| < 1, \\
\frac{1}{2}|k_0 + 2k_3 - m(t_0 + 2t_3)| < \frac{1}{2}m &\iff |t_3 - (\frac{k_0}{2m} + \frac{k_3}{m}\frac{t_0}{2})| < 1.
\end{aligned}$$

Com podem observar, tant t_1, t_2 com t_3 existeixen, ja que en un interval de longitud 2 hi ha com a mínim un nombre enter. Per a la primera equació, aquest enter hi ha casos en que no existeix. Pero podem deixar que la primera component sigui més petita o igual que $\frac{1}{4}m$ i així ens assegurem que existeixi t_0 tal que $|t_0 - \frac{k_0}{m}| \leq \frac{1}{2}$.

Amb aquests t_0, t_1, t_2, t_3 que hem trobat tenim que la norma de $g - qm$ és

$$N(g - qm) < (\frac{1}{16} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4})m^2 < m^2.$$

□

Proposició 4.3. *Siguin α, β enters de Hurwitz, aleshores existeixen $q, \gamma, q', \gamma' \in \mathcal{O}_H$ tals que*

$$\begin{aligned}
\alpha &= q\beta + \gamma \\
\alpha &= \beta q' + \gamma'
\end{aligned} \tag{4.1}$$

amb γ i γ' tals que $N(\gamma), N(\gamma') < N(\beta)$.

Demostració. Considerem el quaternió $g = \alpha\bar{\beta}$ i l'enter $m = N(\beta) = \beta\bar{\beta}$. Per la proposició anterior existeix $q \in \mathcal{O}_H$ tal que $N(g - qm) < m^2$. Així, tenim que

$$g - qm = \alpha\bar{\beta} - q\beta\bar{\beta} = (\alpha - q\beta)\bar{\beta},$$

i per tant,

$$N(g - qm) = N(\alpha - q\beta)N(\bar{\beta}) < N(\beta)N(\bar{\beta}).$$

Sigui $\gamma = \alpha - q\beta$, γ satisfà que $N(\gamma) < N(\beta)$ i

$$\alpha - q\beta = \gamma \Longrightarrow \alpha = q\beta + \gamma.$$

La demostració és anàloga per veure que existeixen $q', \gamma' \in \mathcal{O}_H$ tals que $\alpha = \beta q' + \gamma'$, prenent $g' = \bar{\beta}\alpha$ i $m = \bar{\beta}\beta$. □

La proposició 4.3 no sol ens dóna l'existencia d'un quocient i un residu de la divisió entera de α entre β, sinó que de la demostració podem extreure un algoritme de divisió entera. (El podem trobar a l'annex d'aquest treball.)

4.2 Ideals

A continuació veurem com s'esten la noció d'ideal a aquest anell d'enters. Com que la divisibilitat es diferencia segons per quin costat operem, la definició d'ideal també serà diferent i tindrem dos tipus d'ideals.

Definició 4.3. Diem que un subconjunt no buit I de $\mathcal{O}_H$ és un *ideal per la dreta* si per a tot α i β de I, $\alpha+\beta$ i αq pertanyen a I per a tot $q \in \mathcal{O}_H$.

D'altra banda, diem que I és un *ideal per l'esquerra* si per a tot α i β de I, $\alpha+\beta$ i $q\alpha$ pertanyen a I per a tot $q \in \mathcal{O}_H$.

Teorema 4.1. *L'anell dels enters de Hurwitz és un anell d'ideals principals.*

Demostració. Considerem un ideal $\mathfrak{a}$ per la dreta i δ l'element de $\mathfrak{a}$ de norma mínima. És a dir, que per a tot quaternió γ de l'ideal, si $N(\gamma) < N(\delta)$ aleshores $\gamma = 0$. Sigui $\alpha \in \mathfrak{a}$, aleshores agafant $q \in \mathcal{O}_H$ el quocient de la divisió entera de α entre δ (sabem que existeix per la proposició 4.3), obtenim que

$$N(\alpha - \delta q) < N(\delta) \Longrightarrow \alpha - \delta q = 0 \Longrightarrow \alpha = \delta q.$$

Per tant, tot element de $\mathfrak{a}$ es pot escriure com el producte de δ per un cert enter de Hurwitz q. Aleshores $\mathfrak{a}$ és un ideal principal. El resultat pels ideals per l'esquerra és anàleg. □

A partir d'ara, com que ja sabem que tot ideal de $\mathcal{O}_H$ és principal, escriurem $\delta\mathcal{O}_H$ per indicar els ideals per la dreta i $\mathcal{O}_H\delta$ per indicar els ideals per l'esquerra. Observem que si δ és un quaternió intercanviable, és a dir, $\delta \in \mathcal{O}_H \cup \mathcal{O}_H(1+i)$, aleshores els ideals $\mathcal{O}_H\delta$ i $\delta\mathcal{O}_H$ coincideixen. En aquest cas, direm que els ideals són *bilaterals*.

Definició 4.4. Siguin α i $\beta \in \mathcal{O}_H$, definim el *màxim comú divisor* de α i β per la dreta (resp. esquerra) com l'enter $\delta \in \mathcal{O}_H$ (resp. δ') tal que

$$\mathcal{O}_H\alpha + \mathcal{O}_H\beta = \mathcal{O}_H\delta. \quad (\text{resp. } \alpha\mathcal{O}_H + \beta\mathcal{O}_H = \delta\mathcal{O}_H.)$$

Els notarem de la manera següent.

$$\mathrm{mcd}_d(\alpha,\beta) = \delta, \quad \mathrm{mcd}_e(\alpha,\beta) = \delta'.$$

Observem que existeixen perquè $\mathcal{O}_H$ és un anell d'ideals principals i, per tant, $\mathcal{O}_H\alpha + \mathcal{O}_H\beta$ és un ideal principal i existeix un $\delta \in \mathcal{O}_H$ tal que $\mathcal{O}_H\alpha + \mathcal{O}_H\beta = \mathcal{O}_H\delta$. Anàlogament amb l'ideal $\alpha\mathcal{O}_H + \beta\mathcal{O}_H$. Tal com hem constuit els ideals principals, aquests estan determinats excepte la unitat. Per tant, el $\mathrm{mcd}(\alpha,\beta)$ és únic mòdul producte per unitats de $\mathcal{O}_H^*$.

Observem també que, en particular, $\mathrm{mcd}_d(\alpha,\beta)$ divideix a α i β per la dreta i $\mathrm{mcd}_e(\alpha,\beta)$ divideix a α i β per l'esquerra.

Proposició 4.4 (Identitat de Bézout)**.** *Siguin α i $\beta \in \mathcal{O}_H$ dos enters de Hurwitz no nuls, considerem $\delta = \mathrm{mcd}_d(\alpha, \beta)$ i $\delta' = \mathrm{mcd}_e(\alpha, \beta)$. Aleshores existeixen $p, q, p', q' \in \mathcal{O}_H$ tals que*

$$\delta = p\alpha + q\beta,$$
$$\delta' = \alpha p' + \beta q'.$$

Demostració. De la definició de $\mathrm{mcd}(\alpha, \beta)$ obtenim que

$$\mathcal{O}_H\alpha + \mathcal{O}_H\beta = \mathcal{O}_H\delta$$

$$\alpha\mathcal{O}_H + \beta\mathcal{O}_H = \delta\mathcal{O}_H$$

Aleshores, està clar que existeixen p i $q \in \mathcal{O}_H$ tals que $\delta = p\alpha + q\beta$. I de manera anàloga, existeixen p' i $q' \in \mathcal{O}_H$ tals que $delta = \alpha p' + \beta q'$. □

És natural fer-se la pregunta següent:

Podem establir una relació entre el màxim comú divisor de dos enters i el màxim comú divisor de la seva norma?

En general, no podem contestar a aquesta pregunta. Pero en el cas particular de que α o β siguin intercanviables, sí que podem avançar.

Proposició 4.5. *Sigui $\alpha \in \mathcal{O}_H$ un enter de Hurwitz qualsevol, i $v \in \mathcal{O}_H$ un enter intercanviable. Si les normes de α i v no són coprimeres, aleshores els màxims comuns divisors $\mathrm{mcd}_d(\alpha, v)$ i $\mathrm{mcd}_e(\alpha, v)$ no són unitats. En aquest cas, diem que α i v no són coprimers.*

Demostració. Recordem que els quaternions intercanviables són

$$v = r\varepsilon, \quad \text{i } v = r\zeta\varepsilon.$$

On $r \in \mathbb{Z}$, $\zeta = 1 + i$ i $\varepsilon \in \mathcal{O}_H^*$ és una unitat. Anem a suposar que α i v són coprimers per la dreta (i.e. $\mathrm{mcd}_d(\alpha, v) = \varepsilon \in \mathcal{O}_H$). Aleshores, per la identitat de Bézout, existeixen p i $q \in \mathcal{O}_H$ tals que

$$p\alpha + qv = \varepsilon.$$

Multiplicant per ε^{-1}, obtenim que $p_1\alpha + q_1 v = 1$. Aplicant normes,

$$N(p_1\alpha) = N(\alpha)N(p_1) = N(1-q_1v) = (1-q_1v)(1-\overline{q_1v}) = 1-q_1v-\bar{v}\bar{q_1}-N(v)N(q_1).$$

En el primer cas, si $v = r\varepsilon$, aleshores $N(\alpha)N(p) = 1 - rq\varepsilon - r\bar{\varepsilon}\bar{q} + r^2N(q)$. Dividint l'equació per l'esquerra per un factor primer més gran que 1, que divideixi a $N(\alpha)$ i $N(v) = r^2$ (existeix ja que $\mathrm{mcd}(N(\alpha), N(v)) > 1$), obtenim que aquest ha de dividir a 1. Contradicció.

En segon cas, si $v = r\zeta\varepsilon$, aleshores

$$N(\alpha)N(p_1) = 1 - q_1r(1+i)\varepsilon - r(1-i)\bar{\varepsilon}\bar{q_1} + 2r^2N(q_1).$$

Del fet que $r(1+i)\varepsilon$ és intercanviable, s'obté que existeix $q_2 \in \mathcal{O}_H$ tal que $q_1 r(1+i)\varepsilon = r(1+i)\varepsilon q_2$. Aleshores, podem posar que

$$N(\alpha)N(p_1) = 1 - r(1+i)\varepsilon q_2 + r(1+i)i\bar{\varepsilon}\bar{q_1} + 2r^2 N(q_1).$$

Com que $N(v) = 2r^2$, el màxim comú divisor de $N(\alpha)$ i $N(v)$ conté o bé r o bé $1+i$ com a factors. En el primer cas, dividim l'equació per l'esquerra per r i obtenim que r divideix a 1. En el segon cas, dividim l'equació per la dreta per $1+i$ i obtenim que $1+i$ divideix a 1. Ambdós situacions són contradiccions, per tant, podem concloure que α i v no són coprimers.

□

Definició 4.5. Diem que dos enters α i $\beta \in \mathcal{O}_H$ són *associats* per la dreta (resp. esquerra) si existeix una unitat $\varepsilon \in \mathcal{O}_H$ tal que

$$\alpha = \beta\varepsilon, \quad (\text{ resp. } \alpha = \varepsilon\beta).$$

5 Congruències

En aquesta secció estendrem la noció de congruència que coneixem a $\mathbb{Z}$ als enters de Hurwitz. Per fer-ho ens restringirem al grup dels quaternions intercanviables, estudiats en la secció anterior. També estudiarem les classes de restes mòdul aquests quaternions i farem classificacions dels enters segons les classes on pertanyin.

Definició 5.1. Donat v un quaternió intercanviable, diem que dos enters $\alpha, \beta \in \mathcal{O}_H$ són *congruents mòdul* v quan $a - b$ és múltiple de v. I aleshores, escriurem que

$$\alpha \equiv \beta \pmod{v}.$$

Notem que com que fem congruències mòdul quaternions intercanviables, ser múltiple de v significa ser-ho per la dreta i per l'esquerra. És a dir, si $\alpha - \beta$ és múltiple de v, existeixen g i $h \in \mathcal{O}_H$ tals que

$$a - b = gv,$$
$$a - b = vh.$$

Per tant, no diferenciarem si la congruència és d'esquerres o de dretes. Obtenim així una relació d'equivalència.

Recordem que els quaternions intercanviables són

$$v = r\varepsilon, \quad v = r\zeta\varepsilon,$$

amb r un nombre enter, $\zeta = 1 + i$ i ε una unitat de $\mathcal{O}_H$. Començarem estudiant les congruències mòdul $\zeta = 1 + i$.

5.1 L'anell quocient $\mathcal{O}_H/(1+i)\mathcal{O}_H$

Proposició 5.1. *Els quaternions*

$$0, 1, \rho, \rho^2 = \rho - 1,$$

on $\rho = \frac{1+i+j+k}{2}$*, formen un sistema complet de representants de les classes d'equivalència mòdul* $\zeta = 1 + i$*.*

Demostració. Primer de tot, observem que $1 \equiv i \equiv j \equiv k \pmod{1+i}$. En efecte,

$$i - 1 = i(1+i) \Rightarrow i \equiv 1 \pmod{1+i},$$
$$j - 1 = \frac{-1+i+j+k}{2}(1+i) \Rightarrow j \equiv 1 \pmod{1+i},$$
$$k - 1 = \frac{-1+i-j+k}{2}(1+i) \Rightarrow k \equiv 1 \pmod{1+i}.$$

Sigui $g = k_0\rho + k_1 i + k_2 j + k_3 k$, aleshores pel que acabem de veure, $g \equiv k_0\rho + k_1 + k_2 + k_3 \pmod{1+i}$. A més, del fet que $(1+i)(1-i) = 2$ obtenim que

$$k_1 + k_2 + k_3 \equiv \begin{cases} 0 \pmod{1+i}, & \text{si } k_1 + k_2 + k_3 \text{ és parell,} \\ 1 \pmod{1+i}, & \text{si } k_1 + k_2 + k_3 \text{ és senar.} \end{cases}$$

Equivalentment,

$$k_0\rho \equiv \begin{cases} 0 \pmod{1+i}, & \text{si } k_0 \text{ és parell,} \\ \rho \pmod{1+i}, & \text{si } k_0 \text{ és senar.} \end{cases}$$

Per tant, g és equivalent mòdul $\zeta = 1+i$ amb un dels quatre enters de Hurwitz següents:

$$0, \quad 1, \quad \rho, \quad 1+\rho.$$

Podem canviar $1+\rho$ per ρ^2 ja que si un enter $g \equiv 1+\rho \pmod{1+i}$ aleshores, del fet que $\rho^2 = \rho - 1 = (\rho+1) - 2$, s'obté que $g \equiv 2+\rho^2 \pmod{1+i} \equiv \rho^2 \pmod{1+i}$.

□

Observem que, amb aquesta classificació de les classes de restes mòdul ζ, obtenim que un enter $g \in \mathcal{O}_H$ té les compontents enteres si i només si g és congruent amb 0 o 1 mòdul ζ.

Observació 6. L'anell $\mathcal{O}_H/(1+i)$ és el cos finit $\mathbb{F}_4$. En efecte, tots els elements de $\mathcal{O}_H/(1+i)$ són invertibles excepte el 0, i també es té que $(\mathcal{O}_H/(1+i))^* \cong C_3$.

Proposició 5.2. *Siguin $\alpha \in \mathcal{O}_H$ i r el minim enter tal que 2^r divideix $N(\alpha)$. Aleshores es té que*

$$\alpha = (1+i)^r \beta$$

on β és de $\mathcal{O}_H$, amb norma senar i coprimer amb $(1+i)$.

Demostració. Observem que, en general, si les normes de dos enters de Hurwitz α_1 i $\alpha_2 \in \mathcal{O}_H$ són coprimeres, aleshores α_1 i α_2 són també coprimers. És a dir, α_1 no divideix ni és divisible per α_2 per la dreta ni per l'esquerra. En efecte, suposem per exemple que α_2 divideix per la dreta a α_1, aleshores es té que per un cert $q \in \mathcal{O}_H$

$$\alpha_1 = q\alpha_2 \Longrightarrow N(\alpha_1) = N(q)N(\alpha_2).$$

Per tant, $N(\alpha_2)$ divideix a $N(\alpha_1)$ i no són coprimeres.

Ara bé, considerem $\alpha \in \mathcal{O}_H$ i $\zeta = 1+i$, amb $N(\zeta) = 2$. Volem veure que $\alpha = (1+i)^r\beta$, on r és la potència màxima de 2 que divideix a la norma de α. El cas que $r = 0$ és directe amb l'observació inicial, ja que si $N(\alpha)$ és senar, és coprimera amb la norma de $1+i$ i es té que α és coprimer amb $1+i$. Per $r \geq 0$ ho farem per inducció.

Si $r = 1$ aleshores $N(\alpha)$ és parell. Utilitzant la proposició 5.1 i alguns càlculs, anem a veure que $1+i$ divideix α.

$$\begin{aligned}
\alpha \equiv 1 \pmod{1+i} \Rightarrow & \alpha - 1 = q(1+i) \Rightarrow N(\alpha-1) \text{ és parella,} \\
& N(\alpha-1) = (\alpha-1)(\overline{\alpha}-1) = N(\alpha) - 2Re(\alpha) + 1 \notin 2\mathbb{Z}, \\
\alpha \equiv \rho \pmod{1+i} \Rightarrow & \alpha - \rho = q(1+i) \Rightarrow N(\alpha-\rho) \text{ és parella,} \\
& N(\alpha-\rho) = (\alpha-\rho)(\overline{\alpha}-\overline{\rho}) = N(\alpha) - 2Re(\rho\overline{\alpha}) + 1 \notin 2\mathbb{Z}, \\
\alpha \equiv \rho^2 \pmod{1+i} \Rightarrow & \alpha - \rho^2 = q(1+i) \Rightarrow N(\alpha-\rho^2) \text{ és parella,} \\
& N(\alpha-\rho^2) = (\alpha-\rho^2)(\overline{\alpha}-\overline{\rho^2}) = N(\alpha) - 2Re(\rho^2\overline{\alpha}) + 1 \notin 2\mathbb{Z}.
\end{aligned}$$

Aleshores $\alpha \equiv 0 \pmod{1+i}$ i existeix un enter $\beta \in \mathcal{O}_H$ tal que

$$\alpha = (1+i)\beta.$$

A més, com que teníem que $N(\alpha) = 2k$, on k és un nombre senar, aleshores $N(\beta) = N(\alpha)/2 = k$ és senar. A més, per l'observació inicial, si $N(\beta)$ és senar, β és coprimer amb $1+i$.

En general, considerem $r \leq 2$. Repetint l'argument del cas $r = 1$ es té que si $N(\alpha)$ és parella aleshores $1+i$ divideix a α i existeix un $\alpha_1 \in \mathcal{O}_H$ tal que

$$\alpha = (1+i)\alpha_1.$$

Ara bé, $N(\alpha_1) = N(\alpha)/2 = 2^{r-1}k$. Aplicant la hipòtesi d'inducció a α_1 s'obté que $\alpha_1 = (1+i)^{r-1}\beta$ per un cert $\beta \in \mathcal{O}_H$ coprimer amb $1+i$. Finalment,

$$\alpha = (1+i)^r\beta,$$

i β satisfà que és coprimer amb $1+i$ i $N(\beta) \notin 2\mathbb{Z}$.

□

Aquest resultat ens dóna un criteri per classificar els enters de Hurwitz segons la paritat de la seva norma.

Definició 5.2. Diem que un enter de Hurwitz α és *parell* (resp. *senar*) si la seva norma norma $N(\alpha)$ és parella (resp. senar).

En termes d'enters parells i senars, la proposició anterior es tradueix en:

$$\alpha \text{ senar} \iff \alpha \text{ coprimer amb } 1+i.$$

$$\alpha \text{ parell} \iff \alpha \text{ és divisible per } 1+i.$$

Tot i així, encara podem dir mes del cas en que $N(\alpha) = 2^r\beta$. Si l'exponent r és més gran que 2, aleshores $(1+i)^2 = 2i$ divideix a α i, per tant,

$$\alpha = (1+i)^r\beta = 2i(1+i)^{r-2}\beta.$$

És a dir, α és divisible per 2. Això no té perquè ser cert si $r = 1$.

5.2 L'anell quocient $\mathcal{O}_H/2\mathcal{O}_H$

Procedim ara a estudiar la congruència mòdul $v = 2$.

Proposició 5.3. *Un sistema complet de representants de les classes d'equivalència mòdul 2 és el conjunt format per les 12 unitats*

$$1, \quad i, \quad j, \quad k, \quad \frac{1 \pm i \pm j \pm k}{2}$$

i els quatre enters de Hurwitz

$$0, \quad 1+i, \quad 1+j, \quad 1+k.$$

Demostració. Per fer-ho, reduïm cada una de les coordenades de $g = k_0\rho + k_1 i + k_2 j + k_3 k$ mòdul 2, de tal manera que valguin 0 o 1. Per tant, com a representants de les classes d'equivalència només tenim els 16 quaternions formats per les combinacions de 0 i 1 dels coeficients k_0, k_1, k_2, k_3. Aquests 16 quaternions són, més concretament,

$$\begin{aligned}
&0, \quad i, \quad j, \quad k, i+j, \quad i+k, \quad j+k, \quad i+j+k, \\
&\frac{1+i+j+k}{2}, \quad \frac{1+i+j+3k}{2}, \quad \frac{1+i+3j+k}{2}, \quad \frac{1+3i+j+k}{2}, \\
&\frac{1+i+3j+3k}{2}, \quad \frac{1+3i+j+3k}{2}, \quad \frac{1+3i+3j+k}{2}, \quad \frac{1+3i+3j+3k}{2}.
\end{aligned}$$

Ara bé, observem que

$$\begin{aligned}
&i+j-(1+k) = 2\left(\frac{-1+i+j-k}{2}\right) \Rightarrow i+j \equiv 1+k \pmod 2, \\
&i+k-(1+j) = 2\left(\frac{-1+i-j+k}{2}\right) \Rightarrow i+k \equiv 1+j \pmod 2, \\
&j+k-(1+i) = 2\left(\frac{-1-i+j+k}{2}\right) \Rightarrow j+k \equiv 1+i \pmod 2, \\
&i+j+k-1 = 2\left(\frac{-1+i+j+k}{2}\right) \Rightarrow i+j+k \equiv 1 \pmod 2, \\
&\frac{1+i+j+3k}{2} - \frac{1+i+j-k}{2} = \frac{4k}{2} = 2k \Rightarrow \frac{1+i+j+3k}{2} \equiv \frac{1+i+j-k}{2} \pmod 2.
\end{aligned}$$

Aleshores, si ordenem els 16 representants i apliquem les congruències que acabem de veure, obtenim les 12 unitats

$$1, \quad i, \quad j, \quad k, \quad \frac{1 \pm i \pm j \pm k}{2},$$

i els quatre enters de Hurwitz

$$0, \quad 1+i, \quad 1+j, \quad 1+k.$$

□

Proposició 5.4. *Sigui $\beta \in \mathcal{O}_H$ un quaternió senar, existeix $\varepsilon \in \mathcal{O}_H^*$ unitat tal que es té la congruència*

$$\beta\varepsilon \equiv \varepsilon\beta \equiv 1 \pmod 2.$$

Demostració. Primer de tot, observem que si β és senar, aleshores β és congruent amb una de les 12 unitats $1, i, j, k, \frac{1\pm i\pm j\pm k}{2}$ mòdul 2. En efecte, si suposem que és congruent amb $1+i, 1+j$ o $1+k$, obtenim que

$$\begin{aligned}
&\beta \equiv 1+i \pmod 2 \Rightarrow \beta = (1+i) + 2\gamma = (1+i)(1+(1-i)\gamma), \\
&\beta \equiv 1+j \pmod 2 \Rightarrow \beta = (1+j) + 2\gamma = (1+i)(\frac{1-i+j-k}{2} + (1-i)\gamma), \\
&\beta \equiv 1+k \pmod 2 \Rightarrow \beta = (1+k) + 2\gamma = (1+i)(\frac{1-i+j+k}{2} + (1-i)\gamma),
\end{aligned}$$

obtenint així que $1+i$ divideix a β i, per tant, β no és senar. Sigui $\varepsilon \in \mathcal{O}_H$ la unitat tal que $\beta \equiv \varepsilon \pmod 2$. Aleshores,

$$\beta\varepsilon^{-1} \equiv \varepsilon^{-1}\beta \equiv 1 \pmod 2.$$

□

De la proposició 5.3 s'obté que hi ha 12 enters senars diferents a $\mathcal{O}_H/(2)$. I per la proposició que acabem de veure, aquests són tots invertibles. A més, si $\alpha \equiv, 0, 1+i, 1+j, 1+k \pmod 2$ aleshores α és divisor de 0 i no pot ser invertible. Per tant,

$$\sharp\left(\mathcal{O}_H/2\mathcal{O}_H\right)^* = 12.$$

5.3 Els quaternions primaris

En aquesta secció estudiarem com funciona la congruència mòdul $v = 2(1+i)$. Per fer-ho, utilitzarem els resultats que hem vist fins ara dels anells $\mathcal{O}_H/(1+i)\mathcal{O}_H$ i $\mathcal{O}_H/2\mathcal{O}_H$.

Proposició 5.5. *Donat $\beta \in \mathcal{O}_H$ un quaternió senar, existeixen dos associats de β, β_1 i β_2 tals que*

$$\beta_1, \beta_2 \equiv \begin{cases} 1 \pmod{2(1+i)}, \\ \text{o bé,} \\ 1+2\rho \pmod{2(1+i)}. \end{cases}$$

Demostració. Considerem primer els quaternions congrus amb 1 mòdul 2 i després, utilitzant la proposició 5.4, veurem el resultat per a tots els enters de Hurwitz senars.

Sigui $\alpha \in \mathcal{O}_H$ un enter tal que $\alpha \equiv 1 \pmod 2$. Aleshores, α s'escriu com $1+2g$ per un cert enter $g \in \mathcal{O}_H$. Com que g mòdul $\zeta = 1+i$ només pot ser $0, 1, \rho, \rho^2$, $\alpha = 1+2g$, pot prendre un dels quatre valors següents.

$$1+2\zeta\gamma, \quad 1+2(\zeta\gamma+1), \quad 1+2(\zeta\gamma+\rho), \quad 1+2(\zeta\gamma+\rho^2),$$

per un cert $\gamma \in \mathcal{O}_H$. Per tant, la classe de α mòdul $2(1+i)$ pot ser una de les quatre següents:

$$1, \quad 1+2=-1, \quad 1+2\rho, \quad 1+2\rho^2 = -(1+2\rho).$$

Ara bé, sigui $\beta \in \mathcal{O}_H$ un enter senar qualsevol. Per la proposició 5.4, existeixen ara dos associats de β, $\beta\varepsilon, \varepsilon\beta$ que són congrus amb ± 1 o bé, $\pm(1+2\rho)$ mòdul $2(1+i)$. Per tant, multiplicant ε per -1 si és necessari, podem concloure que existeixen unitats ε_1 i ε_2 tals que

$$\beta\varepsilon_1 \equiv 1 \text{ o bé } 1+2\rho \pmod{2(1+i)},$$

i

$$\varepsilon_2\beta \equiv 1 \text{ o bé } 1+2\rho \pmod{2(1+i)}.$$

□

Definició 5.3. Diem que un enter de Hurwitz $\alpha \in \mathcal{O}_H$ és *primari* si

$$\alpha \equiv 1, \quad \text{o bé} \quad 1 + 2\rho \pmod{2(1+i)}.$$

Corol·lari 5.1. *Tot enter de Hurwitz té un associat per la dreta i un altre per l'esquerra que és primari.*

Proposició 5.6. *El conjunt d'enters de Hurwitz primaris és tancat pel producte.*

Demostració. Siguin $\alpha_1, \alpha_2 \in \mathcal{O}_H$ enters primaris. Aleshores, el producte de α_1 i α_2 és primari, ja que

$$(1+2\rho)^2 - 1 = -3 + 8\rho - 1 = 4(-1+2\rho) = 2(1+i)(1-i)(-1+2\rho).$$

I, per tant, es té que

$$(1+2\rho)^2 \equiv 1 \pmod{2(1+i)}.$$

Aleshores $\alpha_1\alpha_2 \equiv \begin{cases} 1 \pmod{2(1+i)}, \\ \text{ o bé}, \\ 1+2\rho \pmod{2(1+i)}. \end{cases}$ □

Observació 7. Sigui $\alpha \in \mathcal{O}_H$ és un quaternió primari, aleshores si

$$\alpha \equiv 1 \pmod{2(1+i)} \Rightarrow \overline{\alpha} \equiv 1 \pmod{2(1+i)}.$$

En canvi, si $\alpha \equiv 1 + 2\rho \pmod{2(1+i)}$, com que $1 + 2\overline{\rho} = -(1+2\rho)$ es té que

$$-\overline{\alpha} \equiv 1 + 2\rho \pmod{2(1+i)}.$$

Per tant, donat un enter de Hurwitz primari, o bé el seu conjugat o bé l'oposat del conjugat són primaris.

Més endavant, necessitarem treballar amb el conjugat amb un canvi de signe adequat, de tal manera que aquest sigui primari. Per evitar confusions, anomenarem aquest element diferent que el conjugat que coneixem ara.

Definició 5.4. Sigui $\alpha \in \mathcal{O}_H$ primari, definim el seu *conjugat primari* com l'enter α' tal que

$$\begin{aligned} \alpha \equiv 1 \pmod{2+2i} &\implies \alpha' := \overline{\alpha}, \\ \alpha \equiv 1 + 2\rho \pmod{2+2i} &\implies \alpha' := -\overline{\alpha}. \end{aligned} \tag{5.1}$$

Observació 8. Sigui $\alpha \in \mathcal{O}_H$ un enter primari, i sigui $p = N(\alpha) = \alpha\overline{\alpha}$, es pot veure que si α' és el conjugat primari de α, es té que

$$\begin{aligned} \alpha \equiv 1 \pmod{2+2i} &\implies p \equiv 1 \pmod 4, \\ \alpha \equiv 1 + 2\rho \pmod{2+2i} &\implies p \equiv 3 \pmod 4. \end{aligned}$$

Per tant, el conjugat primari satisfà que

$$\alpha' = \left(\frac{-1}{p}\right)\overline{\alpha} = (-1)^{\frac{p-1}{2}}\overline{\alpha}.$$

5.4 L'anell quocient $\mathcal{O}_H/m\mathcal{O}_H$ i els quaternions primitius

Continuem amb l'estudi de la congruència mòdul $v = m \in \mathbb{Z}$, amb m senar. Sigui $g = k_0\rho + k_1 i + k_2 j + k_3 k$. Aleshores podem suposar que, mòdul m, té coordenades enteres ja que

$$g \equiv k_0 m\rho + k_0\rho + k_1 i + k_2 j + k_3 k \pmod{m}.$$

I si m és senar, $1 + m$ és parell i per tant g sempre té un representant mòdul m de coordenades enteres.

Teorema 5.1 (Teorema d'isomorfia)**.** *Siguin $m \in \mathbb{Z}$ senar i $\mathcal{O}_H/m\mathcal{O}_H$ les classes d'equivalència de $\mathcal{O}_H$ mòdul m. Aleshores:*

1. $\#\mathcal{O}_H/m\mathcal{O}_H = m^4$.
2. *Existeix un isomorfisme $\varphi : \mathcal{O}_H/m\mathcal{O}_H \longrightarrow M(2, \mathbb{Z}/m\mathbb{Z})$ tal que*

$$N(g) = \det \varphi(g).$$

Lema 5.1. *Donat un $m \in \mathbb{Z}$ senar, existeixen r i $s \in \mathbb{Z}$ tals que*

$$1 + r^2 + s^2 \equiv 0 \pmod{m}.$$

Demostració. En primer lloc, ho farem per les potències d'un nombre primer. I després, ho estendrem a tot $m \in \mathbb{Z}$ utilitzant la multiplicitat del resultat sobre m.

Part 1: Suposem que $m = p^k$. Ho farem per inducció sobre k.

(i) Suposem que $m = p$ és un nombre primer. Aquest resultat usualment es veu utilitzant el principi del colomar, però nosaltres en mostrarem una demostració alternativa.

Si $p \equiv 1 \pmod 4$ aleshores el símbol de Legendre de -1 val

$$\left(\frac{-1}{p}\right) = 1.$$

Per tant, existeix un $r \in \mathbb{Z}/p\mathbb{Z}$ tal que $r^2 \equiv -1 \pmod p$ i es té que

$$1 + r^2 + 0 \equiv 0 \pmod{p}.$$

Suposem ara que $p \equiv 3 \pmod 4$. Del fet que a $\mathbb{Z}/p\mathbb{Z}$ hi ha el mateix nombre de residus quadràtics que no quadràtics, agafem un element $a \in \mathbb{Z}/p\mathbb{Z}$ que no ho sigui i, en particular, el més petit de tots (és > 0 ja que el 0 és quadràtic). Aleshores:

$$\left(\frac{a}{p}\right) = -1 \Longrightarrow \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = 1.$$

Per tant, existeix un $r \in \mathbb{Z}/p\mathbb{Z}$ tal que $r^2 \equiv -a \pmod p$. Considerem l'element $a - 1$, que com que a és el menor no quadràtic, $a - 1$ ha de ser-ho. Aleshores, existeix un $s \in \mathbb{Z}/p\mathbb{Z}$ tal que $s^2 \equiv a - 1 \pmod p$. Finalment,

$$1 + s^2 \equiv a \equiv -r^2 \pmod{p} \Longrightarrow 1 + r^2 + s^2 \equiv 0 \pmod{p}.$$

(ii) Siguin r_1 i $s_1 \in \mathbb{Z}/p^k\mathbb{Z}$ tals que

$$1 + r_1^2 + s_1^2 \equiv 0 \pmod{p^k}.$$

Considerem els elements $r_2 = r_1 + \lambda p$ i $s_2 = s_1 + \mu p \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ amb $0 \leq \lambda, \mu \leq p-1$. Aleshores,

$$1 + (r_1 + \lambda p)^2 + (s_1 + \mu p)^2 \equiv 1 + r_1^2 + s_1^2 + 2p(\lambda r_1 + \mu s_1) \pmod{p^{k+1}}.$$

Sigui $\nu \in \mathbb{Z}$ tal que $1 + r_1^2 + s_1^2 = \nu p$ aleshores,

$$1 + r_2^2 + s_2^2 \equiv 0 \pmod{p^{k+1}} \Leftrightarrow p(\nu + 2\lambda r_1 + 2\mu s_1) \equiv 0 \pmod{p^{k+1}}.$$

Suposem, sense perdre generalitat, que p^k no divideix a r_1. Aleshores, r_1 és invertible mòdul p^k i si triem λ tal que

$$\lambda \equiv \frac{-\nu - 2s_1\mu}{2r_1} \pmod{p^k},$$

aleshores es té que

$$\nu + 2\lambda r_1 + 2\mu s_1 \equiv 0 \pmod{p^k} \Longrightarrow p(\nu + 2\lambda r_1 + 2\mu s_1) \equiv 0 \pmod{p^{k+1}}.$$

PART 2: Sigui $m = p_1^{r_1} \cdots p_s^{r_s}$ un enter qualsevol. A partir del teorema xinès del residu, s'obté que si r_i, s_i són les solucions de

$$1 + r_i^2 + s_i^2 \equiv 0 \pmod{p_i^{r_i}},$$

aleshores existeixen r i $s \in \mathbb{Z}$ tals que

$$\begin{aligned} r &\equiv r_i \pmod{p_i^{r_i}}, \\ s &\equiv s_i \pmod{p_i^{r_i}}, \end{aligned}$$

per a cada $1 \leq i \leq s$. Així, tenim que

$$1 + r^2 + s^2 \equiv 0 \pmod{m}.$$

□

Demostració Teorema d'isomorfia. 1. Sigui $g = a + bi + cj + dk \in \mathcal{O}_H$, amb $a, b, c, d \in \mathbb{Z}$. Aleshores si fem classe mòdul m de cada una de les components, obtenim m^4 elements possibles. Per tant, hi ha m^4 classes d'equivalència diferents a $\mathcal{O}_H/m\mathcal{O}_H$.

2. Volem definir un morfisme de l'anell $\mathcal{O}_H/m\mathcal{O}_H$ en l'anell de les matrius 2×2 d'entrades a $\mathbb{Z}/m\mathbb{Z}$. Per fer-ho, considerem el parell d'enters r i $s \in \mathbb{Z}$ tals que

$$1 + r^2 + s^2 \equiv 0 \pmod{m}.$$

Definim l'aplicació

$$\varphi : \mathcal{O}_H/m\mathcal{O}_H \longrightarrow M(2, \mathbb{Z}/m\mathbb{Z})$$
$$q \longmapsto \varphi(q),$$

Siguin $q_0, q_1, q_2, q_3 \in \mathbb{Z}$ les coordenades de q, definim els elements $a, b, c, d \in \mathbb{Z}$ de la forma

$$\begin{aligned} a &\equiv q_0 - rq_2 - sq_3 \pmod m, \\ b &\equiv q_0 + rq_2 + sq_3 \pmod m, \\ c &\equiv q_1 - sq_2 + rq_3 \pmod m, \\ d &\equiv q_1 - sq_2 + rq_3 \pmod m. \end{aligned} \tag{5.2}$$

Aleshores, $\varphi(q)$ és la matriu $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Efectivament, $\varphi(q) \in M(2, \mathbb{Z}/m\mathbb{Z})$, i a més no depèn del representant de q ja que si $q = q_0 + q_1 i + q_2 j + q_3 k \equiv \bar{q_o} + \bar{q_1} i + \bar{q_2} j + \bar{q_3} k \pmod m$,

$$\bar{a} = \bar{q_0} - r\bar{q_2} - s\bar{q_3} \equiv q_0 - rq_2 - sq_3 \pmod m \equiv a \pmod m.$$

Anàlogament, es pot comprovar amb b, c i d.

D'altra banda, de 5.2 s'obté que

$$\begin{aligned} 2q_0 &= a + d, \\ 2q_1 &= b - c, \\ 2q_2 &= r(a - d) + s(b + c), \\ 2q_3 &= s(a - d) - r(b + c). \end{aligned}$$

i fent el càlcul de la norma de q en funció de a, b, c i d obtenim que $N(q) \equiv \det \varphi(q) \pmod m$. En efecte,

$$\begin{aligned} N(q) &= \frac{1}{4}((1 + r^2 + s^2)(a^2 + b^2 + c^2 + d^2) + 2ad(1 - r^2 - s^2) - 2bc(1 - r^2 - s^2) + \\ &+ (a - d)(b + c)(2rs - 2rs)) \\ &\equiv \frac{1}{4}(1 - r^2 - s^2)(2ad - 2bc) \pmod m \equiv ad - bc \pmod m. \end{aligned}$$

Només cal veure que és morfisme exhaustiu, perquè utilitzant l'apartat (1) del teorema, el nombre d'elements de $\mathcal{O}_H/m\mathcal{O}_H$ coincideix amb el de $M(2, \mathbb{Z}/m\mathbb{Z})$ i per tant tindrem que φ és isomorfisme.

Donats dos enters de Hurwitz q i $p \in \mathcal{O}_H$ amb imatge

$$\varphi(q) = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad \varphi(p) = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

Aleshores, $\varphi(q + p)$ és una matriu $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tal que

$$\begin{aligned} a &\equiv q_0 + p_0 - r(q_2 + p_2) - s(q_3 + p_3) \pmod m \equiv a_1 + a_2 \pmod m, \\ b &\equiv q_0 + p_0 + r(q_2 + p_2) + s(q_3 + p_3) \pmod m \equiv b_1 + b_2 \pmod m, \\ c &\equiv q_1 + p_1 - s(q_2 + p_2) + r(q_3 + p_3) \pmod m \equiv c_1 + c_2 \pmod m, \\ d &\equiv q_1 + p_1 - s(q_2 + p_2) + r(q_3 + p_3) \pmod m \equiv d_1 + d_2 \pmod m. \end{aligned}$$

Aleshores $\varphi(p+q) \equiv \varphi(p) + \varphi(q) \pmod{m}$.

Per veure que φ respecta el producte, considerem els elements $\xi_1, \xi_2, \xi_3, \xi_4 \in \mathcal{O}_H$ de manera que

$$\begin{aligned}
\xi_1 &= 1 + rj + sk, \\
\xi_2 &= i + sj - rk, \\
\xi_3 &= -i + sj - rk, \\
\xi_4 &= 1 - rj - sk.
\end{aligned}$$

i, observem que es té que si $\varphi(q) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ aleshores

$$2q \equiv a\xi_1 + b\xi_2 + c\xi_3 + d\xi_4 \pmod{m}.$$

Ara bé, siguin $p, q \in \mathcal{O}_H$ enters de Hurwitz amb $\varphi(q) = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ i $\varphi(p) = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$. Enlloc de calcular cada coordenada de qp per trobar la seva imatge, sabem que satisfà:

$$2q2p \equiv (a_1\xi_1 + b_1\xi_2 + c_1\xi_3 + d_1\xi_4)(a_2\xi_1 + b_2\xi_2 + c_2\xi_3 + d_2\xi_4) \pmod{m}.$$

Notem que es tenen les relacions entre els ξ_i següents:

$$\begin{aligned}
&\xi_1^2 \equiv \xi_2\xi_3 \equiv 2\xi_1 \pmod{m}, \\
&\xi_1\xi_2 \equiv \xi_2\xi_4 \equiv 2\xi_2 \pmod{m}, \\
&\xi_3\xi_1 \equiv \xi_4\xi_3 \equiv 2\xi_3 \pmod{m}, \\
&\xi_3\xi_2 \equiv \xi_4^2 \equiv 2\xi_4 \pmod{m}, \\
&\xi_1\xi_3 \equiv \xi_1\xi_4 \equiv 0 \pmod{m} \\
&\xi_2\xi_1 \equiv \xi_2^2 \equiv 0 \pmod{m}, \\
&\xi_3^2 \equiv \xi_3\xi_4 \equiv 0 \pmod{m}, \\
&\xi_4\xi_1 \equiv \xi_4\xi_2 \equiv 0 \pmod{m}.
\end{aligned}$$

Que s'obtenen obtenen de la definició de ξ_1, ξ_2, ξ_3 i ξ_4 i del fet que $1+r^2+s^2 \equiv 0 \pmod{m}$. Ara podem procedir al càlcul de $\varphi(qp)$ amb l'equivalència

$$4qp \equiv (a_1a_2+b_1c_2)2\xi_1+(a_1b_2+b_1d_2)2\xi_2+(c_1a_2+d_1c_2)2\xi_3+(c_1b_2+d_1d_2)2\xi_4 \pmod{m}.$$

Per tant, $\varphi(qp) = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$, satisfent que

$$\varphi(qp) = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \varphi(q)\varphi(p).$$

Observem finalment que φ és un morfisme exhaustiu ja que per a cada matriu $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z}/m\mathbb{Z})$, es pot comprovar que existeix un enter de Hurwitz $q \in \mathcal{O}_H$ tal que $2q \equiv a\xi_1 + b\xi_2 + c\xi_3 + d\xi_4 \pmod{m}$.

□

Notem que la relació definida per les equacions 5.2 preserva el màxim comú divisor dels elements q_0, q_1, q_2 i q_3. És a dir, si $\mathrm{mcd}(q_0, q_1, q_2, q_3) = d$ aleshores $\mathrm{mcd}(a, b, c, d) = d$. Això ens permet definir un tipus de quaternions que podrem identificar o bé amb les seves coordenades, o amb la matriu associada que defineix el morfisme definit en el teorema d'isomorfia.

Definició 5.5. Diem que un enter de Hurwitz $q = q_0 + q_1 i + q_2 j + q_3 k$, $q_0, q_1, q_2, q_3 \in \mathbb{Z}$, és *primitiu* respecte m si $\mathrm{mcd}(q_0, q_1, q_2, q_3, m) = 1$. I diem que una matriu quadrada $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ és primitiva respecte m si $\mathrm{mcd}(a, b, c, d, m) = 1$. Aleshores

Teorema 5.2. *Sigui $m \in \mathbb{Z}$ senar. El nombre de quaternions g primitius respecte m, no congruents mòdul m, tals que*

$$N(g) \equiv 0 \pmod{m}$$

és

$$\psi(m) = m^3 \prod_{p|m} \left(1 - \frac{1}{p^2}\right)\left(1 + \frac{1}{p}\right).$$

Demostració. Aquesta funció aritmètica, $\psi(m)$, també es pot pensar com el nombre de solucions $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ que té l'equació

$$ad - bc \equiv 0 \pmod{m}.$$

Primer de tot, anem a veure que ψ és una funció aritmètica multiplicativa. Siguin $m_1, m_2 \in \mathbb{Z}$ coprimers, i sigui $a_i, b_i, c_i, d_i \in \mathbb{Z}/m_i\mathbb{Z}$ una solució de l'equació

$$ad - bc \equiv 0 \pmod{m_i}$$

per a cada $i = 1, 2$. Aleshores, es té que

$$(a_1 d_1 - b_1 c_1)(a_2 d_2 - b_2 c_2) \equiv 0 \pmod{m_1 m_2}$$

i, per tant, existeix una solució de l'equació $ad - bc \equiv 0 \pmod{m_1 m_2}$ de la forma

$$a = a_1 a_2 + b_1 c_2, \quad b = a_1 b_2 + b_1 d_2, \quad c = a_2 c_1 + d_1 c_2, \quad d = c_1 b_2 + d_1 d_2.$$

Així, per a cada parella de solucions a $\mathbb{Z}/m_1\mathbb{Z}$ i $\mathbb{Z}/m_2\mathbb{Z}$ s'obté una solució a $\mathbb{Z}/m_1 m_2\mathbb{Z}$. Per tant,

$$\psi(m_1 m_2) = \psi(m_1)\psi(m_2).$$

Anem a veure ara com funciona l'equació per una potència k-èsima d'un nombre primer $p \in \mathbb{Z}$ en funció de l'equació en $\mathbb{Z}/p\mathbb{Z}$. Sigui $a_0, b_0, c_0, d_0 \in \mathbb{Z}$ una solució de

$$ad - bc \equiv 0 \pmod{p^k}.$$

Donats $x, y, z, t \in \{0, \ldots, p-1\}$ construïm els elements

$$a = a_0 + p^k x, \quad b = b_0 + p^k y, \quad c = c_0 + p^k y, \quad d = d_0 + p^k t.$$

Aleshores a, b, c i d són solucions de l'equació $ad - bc \equiv 0 \pmod{p^{k+1}}$ si

$$a_0d_0 - b_0c_0 + p^k(a_0t + d_0x - b_0z - c_0y) \equiv 0 \pmod{p^{k+1}}$$

$$\iff \frac{a_0d_0 - b_0c_0}{p^k} + a_0t + d_0x - b_0z - c_0y \equiv 0 \pmod{p}.$$

Per tant, com que havíem considerat $x, y, z, t \in \{0, \ldots, p-1\}$, per a cada x, y i z de 0 a $p-1$ obtenim un t que fa que se satisfaci l'equació anterior i, per tant, hem creat una solució a, b, c, d de l'equació $ad - bc \equiv 0 \pmod{p^{k+1}}$. Així, per a cada solució a $\mathbb{Z}/p^k\mathbb{Z}$ s'obtenen p^3 solucions de l'equació a $\mathbb{Z}/p^{k+1}\mathbb{Z}$. Per tant,

$$\psi(p^{k+1}) = p^3\psi(p^k),$$

i de forma recurrent s'obté que

$$\psi(p^k) = p^{3(k-1)}\psi(p).$$

Per últim, anem a comptar les solucions que té l'equació

$$ad - bc \pmod{p}$$

on $p \in \mathbb{Z}$ és un primer i $a, b, c, d \in \{0, \ldots, p-1\}$, no tots nuls. Observem que si se satisfà l'equació, aleshores es té una de les equivalències següents

$$\begin{aligned} ad \equiv bc \equiv 1 \pmod{p}, \\ ad \equiv bc \equiv 2 \pmod{p}, \\ \vdots \\ ad \equiv bc \equiv p-1 \pmod{p}, \end{aligned} \tag{5.3}$$

o bé,

$$ad \equiv bc \equiv 0 \pmod{p}. \tag{5.4}$$

De 4-tuples que satisfacin una de les equacions del tipus (5.3) n'hi ha $(p-1)^2$ ja que fixant a i b, les altres dues c i d estan fixades. Com que a i b sols es poden moure entre 1 i $p-1$, tenim $(p-1)^2$ possibles solucions.

D'altra banda, per comptar el nombre de solucions que té l'equació (5.4) ho separem en dos casos:

- Contant les que tenen només dos zeros, obtenim $4(p-1)^2$ perque, per exemple, fixant $a = 0$ i $b = 0$, c, d es poden moure de 1 a $p-1$, per tant, n'hi ha $(p-1)^2$.
- Contant les que tenen 3 zeros, obtenim $4(p-1)$ (ja que no pot ser que a, b, c i d siguin nuls simultàniament).

En total, tenim que el nombre de solucions del tipus 5.4 és $4(p-1)^2 + 4(p-1) = 4p^2 - 4p$.

Finalment, si sumem les solucions del tipus (5.3) i (5.4), obtenim que

$$\psi(p) = (p-1)(p-1)^2 + 4p^2 - 4p = (p^2-1)(p+1).$$

Del fet que ψ és una funció aritmètica multiplicativa i que $\psi(p^k) = p^{3(k-1)}\psi(p)$, es té que

$$\psi(m) = m^3 \prod_{p|m} \left(1 - \frac{1}{p^2}\right)\left(1 + \frac{1}{p}\right).$$

□

5.5 L'isomorfisme $\widetilde{A_4} \cong SL(2,3)$

Denotem, com és habitual, per $SL(2,3)$ el grup especial lineal format per les matrius 2×2 de determinant 1 i coeficients en $\mathbb{Z}/3\mathbb{Z}$. A continuació veurem que els quaternions ens permeten obtenir un dels anomenats isomorfismes clàssics.

Teorema 5.3. $\widetilde{A_4} \cong SL(2,3)$.

Lema 5.2. *Sigui $m \in \mathbb{Z}$ senar. El nombre de quaternions g primitius respecte m, no congruents mòdul m tals que*

$$N(g) \equiv 1 \pmod{m}$$

és

$$\chi(m) = m^3 \prod_{p|m} \left(1 - \frac{1}{p^2}\right).$$

Demostració. Aquesta funció aritmètica, $\chi(m)$, també es pot pensar com el nombre de solucions $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ que té l'equació

$$ad - bc \equiv 1 \pmod{m}.$$

Com hem fet en el teorema 5.2, per veure que χ és una funció aritmètica multiplicativa només hem de comprovar que si m_1 i m_2 són coprimers, aleshores dues solucions a_1, b_1, c_1, d_1, i a_2, b_2, c_2, d_2 de les equacions $ad - bc \equiv 1 \pmod{m_i}$ per $i = 1, 2$ proporcionen una solució de $ad - bc \equiv 1 \pmod{m_1 m_2}$. Un cop hem vist que és multiplicativa veiem, de manera idèntica que hem fet abans per ψ, que

$$\chi(p^k) = p^{3(k-1)}\chi(p).$$

(Veure els càlculs en el teorema 5.2.)

Les solucions de $ad - bc \equiv 1 \pmod{p}$ són de la forma

$$\begin{aligned} ad \equiv 2 \pmod{p}, &\quad bc \equiv 1 \pmod{p}, \\ ad \equiv 3 \pmod{p}, &\quad bc \equiv 2 \pmod{p}, \\ &\vdots \\ ad \equiv p-1 \pmod{p}, &\quad bc \equiv p-2 \pmod{p}, \end{aligned} \tag{5.5}$$

o bé,

$$\begin{aligned} ad \equiv 0 \pmod{p}, &\quad bc \equiv p-1 \pmod{p}, \\ ad \equiv 1 \pmod{p}, &\quad bc \equiv 0 \pmod{p}. \end{aligned} \tag{5.6}$$

De 4-tuples que satisfacin una de les equacions del tipus (5.5) n'hi ha $(p-1)^2$ ja que fixant a i b, les altres dues c i d són úniques. Com que a i b sols es poden moure entre 1 i $p-1$, tenim $(p-1)^2$ possibles solucions.

D'altra banda, per comptar el nombre de solucions que tenen les sues equacions (5.5), ho separem en dos casos:

- Les solucions de $bc \equiv p-1 \pmod{p}$ i $ad \equiv 1 \pmod{p}$ són $p-1$.
- Les solucions de $ad \equiv 0 \pmod{p}$ són p de les que $a = 0$ i $0 \leq d \leq p-1$, i $p-1$ de les que $1 \leq a \leq p-1$ i $d = 0$.

Per tant, cada equació de les del tipus (5.5) té $(p-1)(2p-1)$ solucions. Finalment, si sumem les solucions del tipus (5.5) i (5.5), obtenim que

$$\chi(p) = (p-2)(p-1)^2 + 2(p-1)(2p-1) = p(p^2-1).$$

Atès que χ és multiplicativa i que $\chi(p^k) = p^{3(k-1)}\chi(p)$, s'obte que

$$\chi(m) = m^3 \prod_{p|m} \left(1 - \frac{1}{p^2}\right).$$

□

Lema 5.3. *No existeixen dues unitats ε_1 i $\varepsilon_2 \in \mathcal{O}_H^*$ congruents mòdul $m \neq 1$.*

Demostració. Suposem que $\varepsilon_1, \varepsilon_2 \in \mathcal{O}_H^*$ són dues unitats tals que

$$\varepsilon_1 \equiv \varepsilon_2 \pmod{m}.$$

Aleshores, multiplicant per ε_2^{-1} obtenim que

$$\varepsilon := \varepsilon_1 \varepsilon_2^{-1} \equiv 1 \pmod{m}.$$

La única unitat ε que satisfà $\varepsilon \equiv 1 \pmod{m}$ és $\varepsilon = 1$, ja que si $\varepsilon \neq 1$ aleshores

$$\varepsilon - 1 = mg, \text{ per un cert } g \in \mathcal{O}_H \neq 0, \Rightarrow m^2 N(g) \leq 2 \Rightarrow N(g) \leq \tfrac{2}{m^2} < 1.$$

□

Aleshores, el grup de les unitats és un subgrup del conjunt dels $\chi(m)$ quaternions primitius no congruents mòdul m tals que $N(g) \equiv 1 \pmod{m}$.

Demostració del teorema 5.3. El grup de les unitats $\mathcal{O}_H^*$ té 24 elements, i el conjunt dels quaternions primitius no congruents mòdul 3, tals que $N(g) \equiv 1 \pmod{3}$ en té

$$\chi(3) = 3^3(1 - \frac{1}{9}) = 3^3 - 3 = 24.$$

Per tant, els conjunt de representants de les classes d'equivalència de tots els quaternions enters de norma $\equiv 1 \pmod{3}$ són exactaments les 24 unitats $\mathcal{O}_H^*$. Pel

teorema d'isomorfia, aquests representants estan en bijecció amb els elements M de l'anell $M(2, \mathbb{Z}/3\mathbb{Z})$ tals que $\det M \equiv 1 \pmod 3$, que formen el grup $SL(2,3)$, anomenat especial lineal. Havíem vist que

$$\mathcal{O}_H^* \cong \widetilde{A_4},$$

i, per tant,

$$\widetilde{A_4} \cong SL(2,3).$$

□

6 Factorització dels enters de Hurwitz

6.1 Quaternions primers

Definició 6.1. Sigui $\pi \in \mathcal{O}_H$ un enter de Hurwitz. Diem que és un quaternió *primer* si es té que per a tot parell d'enters α i $\beta \in \mathcal{O}_H$ tals que,

$$\pi = \alpha\beta \text{ és } \alpha \in \mathcal{O}_H^* \text{ o bé } \beta \in \mathcal{O}_H^*.$$

6.2 Descomposició de primers de $\mathbb{Z}$ en $\mathcal{O}_H$

Proposició 6.1. *Els nombres primers $p \in \mathbb{Z}$ no són quaternions primers.*

Demostració. El cas en que $p = 2$ és trivial ja que podem descompondre'l en

$$2 = (1 + i)(1 - i),$$

i cap dels factos no és una unitat. Considerem un primer $p \in \mathbb{Z}$ senar i suposem que és un quaternió primer. Considerem un quaternió $g \in \mathcal{O}_H$ coprimer amb p i tal que si $g = k_0 + k_1 i + k_2 j + k_3 k$ aleshores

$$N(g) = k_0^2 + k_1^2 + k_2^2 + k_3^2 \equiv 0 \pmod{p}.$$

Podem considerar-lo perquè a la secció anterior, el teorema 5.2 ens diu que hi ha almenys $\chi(p)$ quaternions amb les seves components coprimeres amb p i tals que $N(g) \equiv 0 \pmod{p}$, i $\chi(p) > 0$ per a tot p. Sigui δ un màxim comú divisor per l'esquerra de p i g. Podem escriure

$$p = \delta\delta_1,$$
$$g = \delta\delta_2,$$

amb $\delta_1, \delta_2 \in \mathcal{O}_H$. Estem suposant que p és un quaternió primer. Per tant, δ_1 ha de ser una unitat. Aleshores tenim que,

$$g = p\delta_1^{-1}\delta_2.$$

Hem arribat a una contradicció, ja que havíem suposat que p i g eren comprimers.

□

Proposició 6.2. *La norma de $\pi \in \mathcal{O}_H$ és un nombre primer si i només si π és un quaternió primer.*

Demostració. Suposem que $N(\pi)$ és primer i que π no és un quaternió primer. És a dir, existeix una descomposició de π

$$\pi = \alpha\beta$$

amb $\alpha, \beta \in \mathcal{O}_H$ no unitats. Si calculem la norma de π obtenim que $N(\pi) = N(\alpha)N(\beta)$. Com que ni α ni β són unitats, $N(\alpha)$ i $N(\beta) \neq 1$. Per tant hem

descompost $N(\pi)$ en dos enters positius i diferents de 1, fet que contradiu que $N(\pi)$ és primer a $\mathbb{Z}$.

Suposem ara que tenim un quaternió primer i considerem un factor primer p de la descomposició de $N(\pi)$ en factors primers. Amb aquestes condicions, π i $\bar{\pi}$ divideix p, suposem que ho fa π sense perdre generalitat ja que si $\bar{p}i$ dividís p acabaríem veient que $N(\bar{\pi}) = p \Rightarrow N(\pi) = p$. Així, tenim que

$$p = \pi\ g$$

per un cert $g \in \mathcal{O}_H$ i en prendre normes obtenim que

$$p^2 = N(\pi)N(g).$$

Per la proposició anterior, p no és un primer a $\mathcal{O}_H$; per tant, g no pot ser una unitat. Per tant, $N(\pi) = p$.

□

Acabem de trobar una manera de cercar tots els quaternions primers de $\mathcal{O}_H$. El que farem a continuació és buscar, per a cada nombre primer p, els quaternions de $\mathcal{O}_H$ de norma p. Farem primer el cas $p = 2$ i la resta la veurem en el teorema 6.1.

Si la norma dels primers que estem buscant és 2, el resultat que mostra la proposició 5.2 aplicada al cas $N(\pi) = 2$ ens diu que π ha de ser de la forma

$$\pi = (1 + i)\varepsilon,$$

on $\varepsilon \in \mathcal{O}_H^*$ és una unitat perquè ha de tenir norma 1. Per tant, hi ha 24 quaternions primers de norma 2, tots ells associats.

Teorema 6.1. *Per a cada nombre primer senar $p \in \mathbb{Z}$, hi ha exactament $p + 1$ enters de Hurwitz, primers i primaris, de norma p.*

Demostració. La demostració d'aquest teorema té dues parts. La primera consisteix en crear un quaternió π primer i primari de norma p a partir d'un enter de Hurwitz que satisfà les condicions del teorema 5.2; és a dir, un enter g no múltiple de p tal que $N(g) \equiv 0 \pmod{p}$. La segona part consisteix en comptar el nombre d'enters g que generen el mateix enter π primer i primari de norma p, i així utilitzant el teorema 5.2, poder comptar quants primers primaris de norma p hi ha.

Part 1: Considerem un enter de Hurwitz $g \in \mathcal{O}_H$, no múltiple de p, tal que

$$N(g) \equiv 0 \pmod{p}.$$

Primer de tot, anem a veure que existeix un altre enter g_1, congruent amb g mòdul p, tal que

$$p \mid N(g_1) \text{ però } p^2 \nmid N(g_1).$$

Suposem que p^2 divideix $N(g)$, ja que en cas contrari ja estaríem. Sigui $g_1 \in \mathcal{O}_H$ de la forma $g_1 = a + bi + cj + dk + p(x + yi + zj + tk)$ per a certs $x, y, z, t \in \mathbb{Z}$. Aleshores la norma de g_1 és

$$N(g_1) = (a + px)^2 + (b + py)^2 + (c + pz)^2 + (d + pt)^2 \equiv$$

$$\equiv a^2 + b^2 + c^2 + d^2 + 2p(xa + yb + zc + td) = 2p(xa + yb + zc + td) \pmod{p^2}.$$

Per exemple, en prendre x, y, z, t tals que $xa+yb+zc+td \equiv 1 \pmod{p}$ ja es té que $N(g_1) \not\equiv 0 \pmod{p^2}$. Per tant, a partir d'ara podem suposar que p^2 no divideix la norma de g.

Considerem π el màxim comú divisor per la dreta de g i p i fem-lo primari multiplicant-lo per una unitat adequada. Per tant, es té que per a un $\alpha \in \mathcal{O}_H$,

$$g = \alpha\pi, \quad p = \pi_1\pi.$$

De la segona equació obtenim que

$$N(\pi) = \begin{cases} 1, \\ p, \\ p^2. \end{cases}$$

L'última opció no es pot donar perquè aleshores aplicant normes a la segona equació tindríem que $N(g)$ és múltiple de p^2. La primera opció, $N(\pi) = 1$ tampoc és possible perquè les normes de g i p no són coprimeres. Per tant, $N(\pi) = p$ i per la proposició 6.2 tenim que π és un quaternió primer. En resum, per a tot enter de Hurwitz $g \in \mathcal{O}_H$ no múltiple de p i tal que $N(g) \equiv 0 \pmod{p}$, existeix un quaternió primer i primari π de norma $N(\pi) = p$.

Part 2: L'objectiu d'aquesta segona part de la demostració és veure que hi ha $p^2 - 1$ enters de Hurwitz g amb les mateixes condicions que a la part 1 tals que el primer primari que generen és el mateix.

Siguin $g_1, g_2 \in \mathcal{O}_H$ no congrus mòdul p, no múltiples de p i tals que $N(g_i) \equiv 0 \pmod{p}$ i $N(g_i) \not\equiv 0 \pmod{p^2}$. Suposem que generen el mateix quaternió primer primari π, és a dir,

$$g_1 = \alpha_1\pi, \quad g_2 = \alpha_2\pi.$$

Observem que $N(\alpha_i)$ és coprimera amb p per a $i = 1, 2$ ja que p^2 no divideix a $N(g_i)$. Considerem un $q \in \mathcal{O}_H$ tal que es té la congruència

$$q\alpha_1 \equiv \alpha_2 \pmod{p}.$$

Multiplicant per π per la dreta, obtenim que

$$qg_1 \equiv g_2 \pmod{p}.$$

Per tant, el conjunt d'enters tals que el quaternió primer i primari que generen és el mateix que un $g \in \mathcal{O}_H$ fixat, són els múltiples de g per l'esquerra, és a dir, qg. El nombre de $q \in \mathcal{O}_H$ no congruents mòdul p és p^4. Anem a veure, per a cada $q \in \mathcal{O}_H$, quants q_i fan que $qg \equiv q_ig \pmod{p}$.

$$qg \equiv q_ig \pmod{p} \Longrightarrow (q - q_i)g \equiv 0 \pmod{p}.$$

Per tant, el nombre de q_i que generen el mateix múltiple de g mòdul p és el nombre de solucions que té l'equació

$$xg \equiv 0 \pmod{p}.$$

Es pot veure que aquest nombre és p^2 (utilitzant el teorema d'isomorfia, el teorema 5.2, i comptant els elements). Aleshores, per a cada enter q, hi ha p^2 q_i tals que $qg \equiv q_i g \pmod{p}$. Per tant, el nombre d'elements de la forma qg per un $q \in \mathcal{O}_H$ no congruents mòdul p és $z = \frac{p^4}{p^2} = p^2$. En suprimir el cas $q = 0$, obtenim que el nombre d'enters que generen el mateix quaternió primer i primari és $p^2 - 1$.

Finalment, anem a la fórmula que ens dóna el teorema 5.2 i obtenim que

$$\psi(p) = (p^2 - 1)(p + 1).$$

Si per a cada g que satisfà les condicions del teorema, hi ha $p^2 - 1$ elements g_i que satisfan també les hipòtesis del teorema que generen el mateix primer π que g, aleshores el nombre de quaternions primers i primaris de norma p no congruents mòdul p és

$$\frac{\psi(p)}{p^2 - 1} = p + 1.$$

□

Aquest resultat és important pel que veurem més endavant a les aplicacions dels enters de Hurwitz en la secció 7. Per calcular de *quantes maneres* es pot escriure un nombre enter com a suma de 4 quadrats.

6.3 Teorema de factorització dels enters de Hurwitz

Anteriorment hem observat que donat un enter α primari, o bé el seu conjugat $\bar{\alpha}$ o bé l'oposat del conjugat $-\bar{\alpha}$ són primaris, i això depèn de si α és 1 o bé $1 + 2\rho$ mòdul $2(1 + i)$. Hem definit aquest element primari com el conjugat primari de α, i l'hem denotat per α'. En aquesta secció necessitarem aquest concepte.

Teorema 6.2 (de factorització)**.** *Sigui $\alpha \in \mathcal{O}_H$ un enter de Hurwitz primitiu, i sigui*

$$N(\alpha) = p_1^{r_1} p_2^{r_2} p_3^{r_3} \cdots p_s^{r_s}$$

la descomposició en factors primers de $N(\alpha)$ tals que $0 < p_1 < p_2 < \cdots < p_s$. Aleshores existeix una única descomposició (mòdul associats) de α en quaternions primers i primaris

$$\alpha = \pi_1^{(1)} \pi_2^{(1)} \cdots \pi_{r_1}^{(1)} \pi_1^{(2)} \cdots \pi_{r_2}^{(2)} \cdots \pi_1^{(s)} \cdots \pi_{r_s}^{(s)}$$

tals que

$$N(\pi_i^{(j)}) = p_j \quad \text{per a tot } 1 \leq j \leq s \text{ i } 1 \leq i \leq r_j.$$

Demostració. Sabem que si la norma de α es descompon com $N(\alpha) = 2^r k$ amb $k \in \mathbb{Z}$ senar, aleshores

$$\alpha = (1 + i)^r \beta,$$

amb β un quaternió senar. A partir d'ara, suposarem que α és senar i si el resultat és cert per enters senars, aleshores per a tot enter $\alpha \in \mathcal{O}_H$ tindrem la descomposició

que estem buscant. Si α no és primari, el podem multiplicar per $\varepsilon \in \mathcal{O}_H^*$ una unitat adequada perquè ho sigui. Així que d'ara en endavant suposarem que α es un enter senar i primari.

Recordem que un enter de Hurwitz $\alpha \in \mathcal{O}_H$ té les coordenades enteres si i només si $\alpha \equiv 0$ o bé $1 \pmod{1+i}$. Si α és primari, aleshores tant si $\alpha \equiv 1 \pmod{2(1+i)}$ com si $\alpha \equiv 1 + 2\rho \pmod{2(1+i)}$ es té que $\alpha \equiv 1 \pmod{1+i}$ i, per tant, té les coordenades enteres.

Considerem $m \in \mathbb{Z}$ el màxim comú divisor de les coordenades de α. Aleshores, podem escriure

$$\alpha = m\gamma,$$

on $\gamma \in \mathcal{O}_H$ és primari i primitiu.

Considerem $\pi_1 \in \mathcal{O}_H$ el màxim comú divisor per l'esquerra de γ i p_1. Aleshores,

$$\gamma = \pi_1\gamma_1,$$

per un cert $\gamma_1 \in \mathcal{O}_H$ primitiu. Multiplicant per una unitat, si cal, agafarem π_1 primari. Observem que si π_1 divideix p, aleshores $N(\pi_1) = p$ i π_1 és primer. Per tant, tenim que

$$N(\gamma) = pN(\gamma_1) \Rightarrow N(\gamma_1) = p_1^{r_1-1}p_2^{r_2}p_3^{r_3}\cdots p_s^{r_s}.$$

Repetint el procés, obtenim el $\pi_2 = \mathrm{mcd}_e(\gamma_1, p_1)$ primer primari de manera que

$$\gamma_1 = \pi_2\gamma_2,$$

amb $\gamma_2 \in \mathcal{O}_H$ i $N(\pi_2) = p_1$. Aleshores,

$$N(\gamma) = p_1^2N(\gamma_2) \Rightarrow N(\gamma_2) = p_1^{r_1-2}p_2^{r_2}p_3^{r_3}\cdots p_s^{r_s}.$$

Finalment, obtindrem $\pi_j^{(i)} \in \mathcal{O}_H$ primers primaris tals que

$$N(\pi_i^{(j)}) = p_j, \quad \text{per a tot } 1 \leq j \leq s,\ 1 \leq i \leq r_j,$$

i γ descompon en la forma

$$\gamma = \pi_1^{(1)}\pi_2^{(1)}\cdots\pi_{k_1}^{(1)}\pi_1^{(2)}\cdots\pi_{k_2}^{(2)}\cdots\pi_1^{(s)}\cdots\pi_{k_r}^{(s)}.$$

□

A la secció 8 podrem trobar una funció que hem creat amb *Mathematica* que factoritza un enter de Hurwitz qualsevol, tot seguint l'algoritme que ens proporciona la demostració d'aquest teorema.

Teorema 6.3. *Siguin $\pi_1, \pi_2, \cdots \pi_s \in \mathcal{O}_H$ quaternions primers i primaris amb $N(\pi_i) = p_i$. Considerem $\alpha \in \mathcal{O}_H$ el producte de tots ells,*

$$\alpha = \pi_1\pi_2\cdots\pi_s.$$

Si es té que per a tot $1 \leq i \leq s-1$, $\pi_i' \neq \pi_{i+1}$, és a dir, no hi ha dos conjugats primaris de costat. Aleshores α és un enter de Hurwitz primitiu.

Demostració. Ho veurem per inducció en el nombre de quaternions primers s. El primer cas és trivial ja que si $\alpha = \pi$ primer i primari, aleshores α és primitiu. A continuació, ho suposem per $s = 1$ i anem a veure que també és cert per s.

Sigui $\gamma = \pi_2\pi_3 \cdots \pi_s$ primitiu, suposem que $\pi_1\gamma = \alpha$ no és primitiu. Existeix un $m \in \mathbb{Z}$ tal que

$$\pi_1\gamma \equiv 0 \pmod{m}.$$

Aleshores,

$$\bar{\pi_1}\pi_1\gamma = p\gamma \equiv 0 \pmod{m}.$$

Com que γ és primitiu, es té que per força $p \equiv 0 \pmod{m}$. Al ser p un nombre primer, obtenim que $p = m$. Aleshores, per un cert $q \in \mathcal{O}_H$ es té que

$$\pi_1\gamma = pq = \pi_1\bar{\pi}_1 q.$$

Per tant, hem trobat una altra descomposició de γ:

$$\gamma = \pi_2 \cdots \pi_s = \bar{\pi_1} q.$$

Pel teorema de factorització anterior, la factorització de γ en factors primers i primaris és única, per tant, π_1 és el conjugat primari de π_2. Però per hipòtesi, no poden haver dos primers π_i i π_j tals que $\pi_2 = \pi_1'$ (el conjugat primari). Per tant, $\alpha = \pi_1\pi_2 \cdots \pi_s$ és primitiu. □

Exemple 9. Donem un exemple de factorització d'un quaternió en producte de quaternions primers i primaris. Els càlculs necessaris es donen a la secció 8.

$$\begin{aligned} 6 - 12i &= (1+i)^2(-6-3i) \\ &= (1+i)^2 3(-2-i) \\ &= (1+i)^2(-i+j+k)^2(2+i) \\ &= (1+i)^2(-i+j+k)^2(-i)(-1+2i). \end{aligned}$$

7 Aplicacions

En aquesta secció presentem dues aplicacions dels quaternions. D'una banda, els quaternions reals ens permeten expressar amb comoditat el grup de les rotacions de $\mathbb{R}^3$ i introduir el grup dels espinors. De l'altra, presentarem una versió quantitativa del teorema de Lagrange segons el qual tot enter és expressable com a suma de quatre quadrats. Els quaternions permeten no solament obtenir aquest resultat de manera natural sinó que, a més, ens proporcionen el nombre de maneres en què podem descompondre qualsevol enter com a suma de quatre quadrats.

7.1 Rotacions de $\mathbb{R}^3$ amb quaternions

Sigui $V := \{x \in \mathbb{H} \mid \bar{x} = -x\}$ l'espai dels quaternions purs. Podem establir una bijecció entre V i $\mathbb{R}^3$ tal que a cada quaternió pur $q = bi + cj + dk$ li assignem el vector de coordenades $(b, c, d) \in \mathbb{R}^3$. El producte de dos quaternions purs u i v pensat a $\mathbb{R}^3$ és

$$uv = -\langle u, v\rangle + (u \wedge v)$$

on $\langle \cdot, \cdot \rangle$ és el producte escalar i $(\cdot \wedge \cdot)$ és el producte vectorial.

Veurem que podem definir qualsevol rotació de $\mathbb{R}^3$ únicament utilitzant un cert quaternió de norma 1.

Lema 7.1. *Sigui $u \in \mathbb{H}$, $N(u) = 1$, existeixen un quaternió pur ε de norma 1 i un angle α de manera que*

$$u = \cos\frac{\alpha}{2} + \sin\frac{\alpha}{2} \cdot \varepsilon$$

Demostració. Posem $u = a + \lambda\varepsilon$ on $a \in \mathbb{R}$ és la part real de u, $\varepsilon \in V$ pur de norma 1 i $\lambda \in \mathbb{R}$. Aleshores,

$$1 = N(u) = a^2 + \lambda^2 N(\varepsilon) = a^2 + \lambda^2.$$

Per tant existeix un $\alpha \in [0, 2\pi)$ tal que

$$\cos\frac{\alpha}{2} = a, \ \sin\frac{\alpha}{2} = \lambda$$

i tenim que $u = \cos\frac{\alpha}{2} + \sin\frac{\alpha}{2} \cdot \varepsilon$. □

Proposició 7.1. *Sigui $u \in \mathbb{H}$, $N(u) = 1$. L'automorfisme intern*

$$\begin{array}{rccc} \varphi_u : & \mathbb{H} & \longrightarrow & \mathbb{H} \\ & q & \longrightarrow & uq\bar{u} = uqu^{-1} \end{array}$$

defineix una rotació de l'espai V dels quaternions purs. Recíprocament, tota rotació de V s'obté d'aquesta manera.

Demostració. Posem $u = \cos\frac{\alpha}{2} + \sin\frac{\alpha}{2} \cdot \varepsilon$, amb $\varepsilon \in V$.

Definim una nova base de l'espai V a partir de ε:

- $\varepsilon_1 = \varepsilon$
- ε_2 un vector ortogonal a ε_2 (és a dir, $\langle \varepsilon_1, \varepsilon_2 \rangle = 0$) i de norma 1.
- I finalment agafem $\varepsilon_3 = (\varepsilon_1 \wedge \varepsilon_2)$.

Sigui $v = x\varepsilon_1 + y\varepsilon_2 + z\varepsilon_3 \in V$ un vector qualsevol. Aleshores:

$$\begin{aligned}\varphi_u(v) = uvu^{-1} = (\cos\frac{\alpha}{2} + \sin\frac{\alpha}{2}\cdot\varepsilon) \quad v \quad (\cos\frac{\alpha}{2} - \sin\frac{\alpha}{2}\cdot\varepsilon) = \\ = x\varepsilon_1 + (y\cos\alpha - z\sin\alpha)\varepsilon_2 + (z\cos\alpha + y\sin\alpha)\varepsilon_3.\end{aligned}$$

I, per tant, podem escriure l'automorfisme φ_u com l'aplicació lineal de $\mathbb{R}^3$ que en la base $\varepsilon_1, \varepsilon_2, \varepsilon_3$ té la matriu següent:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}$$

que correspon a una rotació d'angle α i eix $\varepsilon_1 = \varepsilon$.

Recíprocament, donada una rotació d'angle α i eix ε, posem

$$u = \cos\frac{\alpha}{2} + \sin\frac{\alpha}{2}\varepsilon$$

i per tant fer una rotació d'angle α i eix ε és equivalent a fer $\varphi_u(v) = uvu^{-1}$ per aquest u que hem definit. □

Definició 7.1. Posarem

$$\mathrm{Spin}_3(\mathbb{R}) = \{\alpha \in \mathbb{H} \mid N(\alpha) = 1\}$$

el conjunt dels quaternions de norma 1. $\mathrm{Spin}_3(\mathbb{R})$ és un grup respecte del producte. És l'anomenat *grup dels espinors*.

Proposició 7.2. *Tenim una successió exacta*

$$1 \longrightarrow C_2 \longrightarrow \mathrm{Spin}_3(\mathbb{R}) \xrightarrow{\Phi} SO_3(\mathbb{R}) \longrightarrow 1 \tag{7.1}$$

on $\Phi(u) = \varphi_u$, C_2 *és el grup cíclic d'ordre* 2 *i* $SO_3(\mathbb{R})$ *és el grup de les rotacions de* $\mathbb{R}^3$.

Demostració. Sigui $V = \{\alpha \in \mathbb{H} \mid -\alpha = \bar{\alpha}\}$. Observem que $\varphi_u(v) = uv\bar{u} \in V$, ja que

$$\overline{uv\bar{u}} = u\bar{v}\bar{u} = -uv\bar{u}.$$

Hem vist al teorema anterior que φ_u és una rotació de $\mathbb{R}^3$ i que totes les rotacions de $\mathbb{R}$ s'obtenen es poden escriure com φ_u per un cert $u \in \mathrm{Spin}_3(\mathbb{R})$. Aleshores el morfisme

$$\begin{aligned}\Phi: \quad \mathrm{Spin}_3(\mathbb{R}) &\longrightarrow SO_3 \\ u &\longmapsto \varphi_u\end{aligned} \tag{7.2}$$

està ben definit i és exhaustiu.

Per veure que la successió 7.1 és exacta, només ens cal veure que el nucli de Φ és isomorf a C_2.

Sigui $u \in \mathrm{Spin}_3(\mathbb{R})$, aleshores es té que $N(u) = 1$ i, per tant

$$u^{-1} = \frac{\bar{u}}{N(u)} = \bar{u}.$$

El nucli de Φ està format pels elements u de $\mathrm{Spin}_3(\mathbb{R})$ tals que $\varphi_u = Id_V$. Sigui $\varphi_u \in \mathrm{Ker}(\Phi)$, aleshores per a tot $v \in V$ tenim que

$$uv\bar{u} = v \Longrightarrow uv = vu \Longrightarrow u \in \mathbb{R} \cap \mathrm{Spin}_3(\mathbb{R}) \Longrightarrow N(u) = 1 \text{ i } u \in \mathbb{R} \Longrightarrow u = \pm 1.$$

□

7.2 Sumes de quatre quadrats

Teorema 7.1. *Sigui p un nombre primer, existeixen $8(p+1)$ 4-tuples solucions enteres de l'equació*

$$p = a^2 + b^2 + c^2 + d^2$$

i existeixen $16(p+1)$ 4-tuples solucions senars de l'equació

$$4p = a^2 + b^2 + c^2 + d^2.$$

Demostració. Buscar les representacions de p com a suma de quatre quadrats de $\mathbb{Z}$ és equivalent a buscar enters de Hurwitz de coordenades enteres, que tinguin norma p. Recordem que, pel teorema 6.1, hi ha $p+1$ enters de Hurwitz diferents primers i primaris tals que la seva norma és p. Per a cada enter π d'aquests $p+1$ primers i primaris, tots els seus associats també tenen norma p. Tot i així, no tots els 24 associats són de coordenades enteres. Com que si π és primari, aleshores té coordenades enteres, hi ha 16 associats de la forma

$$\frac{1}{2}(a' + b'i + c'j + d'k),$$

i 8 associats de la forma

$$(a' + b'i + c'j + d'k).$$

Tots ells de norma p. Aleshores, en total hi ha $8(p+1)$ enters de Hurwitz de coordenades enteres i de norma p. I, per tant, un nombre primer p es pot escriure de $8(p+1)$ formes com a suma de quatre quadrats.

D'altra banda, també podem calcular de quantes formes es pot escriure $4p$ com a suma de quatre quadrats senars, utilitzant que hi ha $16(p+1)$ enters de Hurwitz de la forma

$$\frac{1}{2}(a' + b'i + c'j + d'k)$$

i de norma p. Per tant, $N(a' + b'i + c'j + d'k) = 4p$ i aquest nombre és $16(p+1)$. Observem que són solucions senars de l'equació

$$4p = a^2 + b^2 + c^2 + d^2.$$

perquè els quaternions de la forma $\frac{1}{2}(a+bi+cj+dk)$ tals que no totes les coordenades a, b, c i d són senars, no són enters de Hurwitz. □

Volem estendre el resultat per a tot nombre natural $n \in \mathbb{N}$ i trobar de quantes maneres es pot escriure un nombre natural com a suma de quatre quadrats. Per fer-ho necessitem alguns resultats previs.

Lema 7.2. *Si $n \in \mathbb{N}$ és un nombre senar, el nombre de quaternions primaris de norma n és*

$$S(n) = \sum_{d|n} d.$$

Demostració. En primer lloc, obtindrem el nombre de quaternions primaris i primitius de norma n i més endavant, considerarem els quaternions que no són primitius i així, obtindrem el nombre total de quaternions primaris de norma n.

Pel teorema 6.1 s'obté que si $n = p$ primer, aleshores el nombre d'enters de Hurwitz primaris i primitius de norma p és $p+1$. Dels teoremes 6.3 i 6.2 obtenim que, si $n = p^r$ aleshores el nombre d'enters de Hurwitz primitius i primaris és

$$(p+1)p^{r-1}$$

En efecte, el teorema 6.3 ens diu que un producte de quaternions primers i primaris

$$\pi_1\pi_2\cdots\pi_s$$

és primitiu si no hi ha conjugats primaris de costat. Aleshores, el primer π_1 pot ser de $(p+1)$ maneres diferents, però la resta de primers π_i no poden ser el conjugat primari de π_{i-1}, per tant, només poden ser escollits de p maneres diferents.

En general, si $n = p_1^{r_1}\cdots p_s^{r_s}$ es té que el nombre de quaternions primaris i primitius de norma n és

$$S_1(n) = (p_1+1)p_1^{r_1-1}\cdots(p_s+1)p_s^{r_s-1}.$$

Sigui $\alpha \in \mathcal{O}_H$ un enter de Hurwitz primari no primitiu. Aleshores, diem d al màxim comú divisor de les seves coordenades i obtenim que,

$$\alpha = d\beta,$$

on $\beta \in \mathcal{O}_H$ primari i primitiu amb $N(\beta) = \frac{n}{d^2}$. Pel que hem vist abans, per a cada divisor d^2 de n, tenim $S_1(\frac{n}{d^2})$ quaternions primaris de norma n. Aleshores, en total tenim

$$S(n) = \sum_{d^2|n} S_1(\frac{n}{d^2})$$

quaternions primaris de norma n.

Finalment, per veure

$$\sum_{d^2|n} S_1(\frac{n}{d^2}) = \sum_{d|n} d,$$

ens podem restringir al cas $n = p^r$ amb p primer, ja que la suma dels divisors d'un nombre està clar que és una funció aritmètica multiplicativa. Suposem que $n = p^r$. Si $d^2 \mid p^r$, aleshores $d^2 = p^{2k}$ amb $2k \leq r$. Per tant,

$$S(p) = \sum_{k=1}^{r/2} S_1(p^{r-2k}) = (p+1)p^{r-1} + (p+1)p^{r-3} + \cdots = p^r + p^{r-1} + \cdots + p + 1 = \sum_{d|p} d.$$

□

Teorema 7.2. *El nombre de total de formes en què un nombre $n \in \mathbb{N}$ es pot posar com la suma de quatre quadrats és 8 vegades la suma dels seus divisors si n és senar i 24 vegades la suma dels seus divisors senars, si n és parell. És a dir, si diem $r_4(n)$ al nombre de formes en què n s'escriu com la suma de quatre quadrats, aleshores*

$$r_4(n) = \begin{cases} 8 \displaystyle\sum_{d|n} d & \text{si } n \text{ és senar,} \\ 24 \displaystyle\sum_{\substack{d|n \\ d \not\equiv 0 (\bmod 2)}} d & \text{si } n \text{ és parell.} \end{cases}$$

Demostració. Tal i com hem observat en el teorema 7.1, el nombre de formes en què un nombre n s'escriu com a suma de quatre quadrats enters és el mateix que el nombre de quaternions de coordenades enteres de norma n.

Cas 1: Si n és senar, pel lema 7.2 el nombre de quaternions de coordenades enteres, primaris i de norma n és

$$S(n) = \sum_{d|n} d.$$

Per a cada enter de Hurwitz primari, hi ha 7 associats que també tenen les coordenades enteres (multiplicant per les unitats $\pm i, \pm j, \pm k, -1$). Els 16 associats restants no tenen les components enteres. Per tant, si n és senar és té que n es pot p

$$r_4(n) = 8 \sum_{d|n} d.$$

Cas 2: Suposem ara que n és parell. Sigui 2^r la màxima potència de 2 que divideix n, es té que tot enter de Hurwitz α de norma n s'escriu en la forma

$$\alpha = (1+i)^r \beta,$$

on $\beta \in \mathcal{O}_H$ un quaternió senar de norma $N(\beta) = \frac{n}{2^r}$. Observem que tot enter $\alpha \in \mathcal{O}_H$ que sigui divisible per l'esquerra per $1+i$ té coordenades enteres. En efecte,

$$\alpha = (1+i)\frac{1}{2}(a + bi + cj + dk) = \frac{a - b + (a+b)i + (c-d)j + (c+d)k}{2}$$

té les coordenades enteres ja que $\frac{1}{2}(a+bi+cj+dk) \in \mathcal{O}_H$ si a, b, c i d són tots parells o tots senars i, per tant, $a+b, a-b, c+d, c-d$ són nombres parells.

Per tant, cada enter $\beta \in \mathcal{O}_H$ de norma $\frac{n}{2^r}$ ens dóna un enter α de norma n i de coordenades enteres. Si contem el nombre d'enters β de norma $\frac{n}{2^r}$ ja estarem. Per cada quaternió primari hi ha 24 associats diferents. Per tant, el nombre d'enters β de norma n és 24 vegades el nombre de quaternions primaris amb aquesta norma. Atès que el lema 7.2 ens dóna el nombre de quaternions primaris d'una certa norma, obtenim que

$$r_4(n) = 24 \sum_{d \mid \frac{n}{2^r}} d = 24 \sum_{\substack{d \mid n \\ d \not\equiv 0 (\bmod 2)}} d.$$

□

Observem que aquest resultat en el cas que $n = p$ és un nombre primer coincideix amb el que hem vist en el teorema 7.1 ja que la suma dels divisors d'un nombre primer és $p+1$.

A la secció següent, podrem trobar un algoritme que calcula totes les formes d'escriure un nombre natural com a suma de quatre quadrats. Equivalentment, l'algoritme que veurem també proporciona tots els enters de Hurwitz de coordenades enteres d'una certa norma. Podrem comprovar el teorema 7.2 per a nombres naturals petits.

Divisió entera de quaternions

A la secció 4.1 del treball hem trobat un algoritme per fer la divisió entera entre dos enters de Hurwtiz qualsevols. Per implementar l'algoritme al Matemàtica, hem necessitat algunes funcions que ens proporciona el paquet dels Quaternions, que són les següents.

- **`**`**: És el símbol que s'utilitza per fer el producte de dos quaternions (no s'utilitza `*` perquè el producte no és commutatiu).
- **`Conjugate[a]`**: Calcula el conjugat d'un quaternió `a`.
- **`Norm[a]`**: Calcula la norma del quaternió `a`.
- **`Round[a]`**: Calcula l'enter de Hurwitz que està més proper a `a`, és a dir, busca l'enter de Hurwitz tal que la norma de `Round[a]-a` és mínima.

Primer de tot, introduim el paquet dels Quaternions del Matemàtica.

In[76]:=
```
<< Quaternions`
```

La divisió entera per la dreta de dos enters de Hurwitz `a` i `b` consisteix en trobar `q` i `r` enters de Huwritz tals que `a=qb + r` i la norma de `r` sigui menor que la de `b`. L'algoritme que mostrarem a continuació és el que fa servir la demostració de la proposició 4.3 per provar l'existència dels elements `q` i `r`.

In[77]:=
```
QuocientDreta[a_, b_] := Round[a ** Conjugate[b] / Norm[b]]
                         entero más ··· conjugado  norma
```

In[78]:=
```
ResiduDreta[a_, b_] := a - Round[a ** Conjugate[b] / Norm[b]] ** b
                       entero más ··· conjugado  norma
```

In[79]:=
```
DivisioEnteraDreta[a_, b_] := {QuocientDreta[a, b], ResiduDreta[a, b]}
```

In[80]:=
```
a = Quaternion[1, -3, 4, -2]
b = Quaternion[1/2, 3/2, 5/2, -1/2]
{q1, r1} = DivisioEnteraDreta[a, b]
```

Out[80]=
$$\text{Quaternion}[1, -3, 4, -2]$$

Out[81]=
$$\text{Quaternion}\left[\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, -\frac{1}{2}\right]$$

Out[82]=
$$\left\{\text{Quaternion}\left[\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}\right], \text{Quaternion}\left[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right]\right\}$$

In[83]:=
```
a == q1 ** b + r1
```

Out[83]=
```
True
```

La divisió entera per l'esquerra es fa d'una manera semblant, i troba els enters de Hurwitz `q` i `r` tals que se satisfà `a=bq + r`.

In[84]:=
```
QuocientEsquerra[a_, b_] := Round[Conjugate[b] ** a / Norm[b]]
                            enter··· conjugado  norma
```

In[85]:=
```
ResiduEsquerra[a_, b_] := a - b ** Round[Conjugate[b] ** a / Norm[b]]
                          enter··· conjugado  norma
```

In[86]:=
```
DivisioEnteraEsquerra[a_, b_] := {QuocientEsquerra[a, b], ResiduEsquerra[a, b]}
```

In[87]:=
```
{q2, r2} = DivisioEnteraEsquerra[a, b]
```

Out[87]=
$$\left\{\text{Quaternion}\left[\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{3}{2}\right], \text{Quaternion}[1, 0, 1, 1]\right\}$$

In[88]:=
```
a == b ** q2 + r2
```

Out[88]=
```
True
```

Suma de quatre quadrats

Anteriorment hem vist que tot nombre natural el podem escriure de 8 vegaddes la suma dels seus divisors si és senar, i 24 vegades la suma dels seus divisors senars, si és parell. A coninuació, escriurem totes les maneres possibles que hi ha d'escriure i comprovarem amb alguns exemples que se satisfà el teorema que ens dóna r_4.

Les funcions que farem servir a continuació són:

- **`Quaternion[a,b,c,d]`**: Escriu el quaternió de coordenades a, b, c, d. És a dir, a + bi + cj dk.
- **`Norm[q]`**: Calcula la norma del quaternió q.

A continuació, definirem tre funcions, la primera **`Llista[p]`** escriu una taula amb la norma dels quaternions que tenen coordenades més petites que l'arrel de **`p`**, en valor absolut. La segona funció, **`Quadrats[p]`**, agafa els elements de la Llista[p] que són exactament **`p`**, i en troba la posició. Aquesta posició són les coordenades **`x,y,z,t`** del quaternió que té norma p. Per tant, la funció **`Quadrats[p]`** escriu tots els quaternions de coordenades enteres de norma **`p`**. Per últim, com que el nombre de quaternions creix considerablement, contarem quants quaternions de coordenades enteres i de norma **`p`** hi ha.

In[89]:=
```
Llista[p_] := Table[Norm[Quaternion[x, y, z, t]],
                    tabla   norma
  {x, Ceiling[-Sqrt[p]], Sqrt[p]}, {y, Ceiling[-Sqrt[p]], Sqrt[p]},
      entero supe··  raíz cuadrada  raíz cuadrada   entero supe··  raíz cuadrada  raíz cuadrada
  {z, Ceiling[-Sqrt[p]], Sqrt[p]}, {t, Ceiling[-Sqrt[p]], Sqrt[p]}]
      entero supe··  raíz cuadrada  raíz cuadrada   entero supe··  raíz cuadrada  raíz cuadrada
```

In[90]:=
```
Quadrats[p_] := Position[Llista[p], p] - Floor[Sqrt[p]] - 1
                  posición              entero···  raíz cuadrada
```

In[91]:=
```
NombreQuadrats[p_] := Length[Quadrats[p]]
                      longitud
```

Vegem primer alguns exemples amb **`p`** primer. Per un resultat vist al treball, el nombre de quaternions de coordenades enteres de norma **`p`** és **`8(p+1)`**, anem a comprovar-ho.

In[92]:=
```
Quadrats[2]
```

Out[92]=
```
{{-1, -1, 0, 0}, {-1, 0, -1, 0}, {-1, 0, 0, -1}, {-1, 0, 0, 1},
 {-1, 0, 1, 0}, {-1, 1, 0, 0}, {0, -1, -1, 0}, {0, -1, 0, -1}, {0, -1, 0, 1},
 {0, -1, 1, 0}, {0, 0, -1, -1}, {0, 0, -1, 1}, {0, 0, 1, -1}, {0, 0, 1, 1},
 {0, 1, -1, 0}, {0, 1, 0, -1}, {0, 1, 0, 1}, {0, 1, 1, 0}, {1, -1, 0, 0},
 {1, 0, -1, 0}, {1, 0, 0, -1}, {1, 0, 0, 1}, {1, 0, 1, 0}, {1, 1, 0, 0}}
```

In[93]:=
```
NombreQuadrats[2]
```

Out[93]=
```
24
```

El nombre d'elements que ens apareix és **24**, que efectivament coincideix amb **8(2+1)**.

In[94]:=
```
Quadrats[3]
```

Out[94]=
```
{{-1, -1, -1, 0}, {-1, -1, 0, -1}, {-1, -1, 0, 1}, {-1, -1, 1, 0},
 {-1, 0, -1, -1}, {-1, 0, -1, 1}, {-1, 0, 1, -1}, {-1, 0, 1, 1},
 {-1, 1, -1, 0}, {-1, 1, 0, -1}, {-1, 1, 0, 1}, {-1, 1, 1, 0}, {0, -1, -1, -1},
 {0, -1, -1, 1}, {0, -1, 1, -1}, {0, -1, 1, 1}, {0, 1, -1, -1},
 {0, 1, -1, 1}, {0, 1, 1, -1}, {0, 1, 1, 1}, {1, -1, -1, 0}, {1, -1, 0, -1},
 {1, -1, 0, 1}, {1, -1, 1, 0}, {1, 0, -1, -1}, {1, 0, -1, 1}, {1, 0, 1, -1},
 {1, 0, 1, 1}, {1, 1, -1, 0}, {1, 1, 0, -1}, {1, 1, 0, 1}, {1, 1, 1, 0}}
```

In[95]:=
```
NombreQuadrats[3]
```

Out[95]=
```
32
```

El nombre d'elements que ens apareix és **32**, que efectivament coincideix amb **8(3+1)**.

In[96]:=
```
NombreQuadrats[5]
```

Out[96]=
```
48
```

El nombre d'elements que ens apareix és **48**, que efectivament coincideix amb **8(5+1)**.

Ara anem a comprovar, amb alguns exemples, que el nombre de quaternions de coordenades enteres i de norma un nombre senar és **8** vegades la suma dels seus divisors.

In[97]:=
```
NombreQuadrats[9] == 8 * DivisorSum[9, # &]
                     suma de divisores
```

Out[97]=
```
True
```

In[98]:=
```
NombreQuadrats[51] == 8 * DivisorSum[51, # &]
                     suma de divisores
```

Out[98]=
```
True
```

In[99]:=
```
NombreQuadrats[195] == 8 * DivisorSum[195, # &]
                     suma de divisores
```

Out[99]=
```
True
```

Finalment, comprovem amb alguns exemples que el nombre de quaternions de coordenades enteres i de norma un nombre parell és **24** vegades la suma dels seus divisors senars.

In[100]:=
```
NombreQuadrats[6] == 24 * DivisorSum[6 / 2^IntegerExponent[6, 2], # &]
                     suma de divisores   exponente entero
```

Out[100]=
```
True
```

```
In[101]:= NombreQuadrats[92] == 24 * DivisorSum[92 / 2^IntegerExponent[92, 2], # &]
                                  suma de divisores   exponente entero
Out[101]= True

In[102]:= NombreQuadrats[128] == 24 * DivisorSum[128 / 2^IntegerExponent[128, 2], # &]
                                   suma de divisores   exponente entero
Out[102]= True
```

Factorització dels enters de Hurwitz

A la demostració del Teorema de Factorització de la secció 6.3 hem vist un algoritme per factoritzar un enter de Hurwitz en quaternions primers. Hem necessitat l'ajuda d'algunes funcions que ens proporciona el Matemàtica, que són les següents.

- **`Re[q]`:** Proporciona la part real del quaternió `q`.
- **`RightGCD[p,q]`:** Calcula el màxim comú divisor per la dreta de dos quaternions `p` i `q`.
- **`UnitQuaternions`:** És la llista de les 24 unitats de l'anell dels enters de Hurwitz.
- **`Mod[p,q]`:** És la representació de `p` a l'anell de classes a $O_H/(q)\,O_H$.

L'algoritme utilitza algunes reduccions per arribar a descompondre un enter de Hurwitz qualsevol, a un que sigui primari i primitiu. Per fer aquestes reduccions, hem definit dues funcions auxiliars que són les següents.
La primera, `FactorComu[q]`, calcula el màxim comú divisor de les components d'un quaternió. Vegem també un exemple.

```
In[103]:= FactorComu[q_] := GCD[Re[q], Re[-Quaternion[0, 1, 0, 0] ** q],
                              má··· parte r··· parte real
   Re[-Quaternion[0, 0, 1, 0] ** q], Re[-Quaternion[0, 0, 0, 1] ** q]]
   parte real                        parte real

In[104]:= a = Quaternion[2, 4, 6, -2]
          FactorComu[a]
Out[104]= Quaternion[2, 4, 6, -2]

Out[105]= 2
```

La segona funció calcula l'enter associat per l'esquerra a `q` que és primari (recordem que aquest associat primari existeix si `q` és senar). És a dir, si `p=AssociatPrimari[q]`, aleshores `q=ep` per una certa unitat `e` i, a més, `p` és un enter primari. Per fer-ho, recorre tots els associats per l'esquerra de `q` fins que hi ha un que és o bé `1` o bé `1 + 2` $\left(\frac{1+i+j+k}{2}\right)$ mòdul `2(1+i)`. Durant la construcció d'aquesta funció, hem vist que els operadors `==` i `!=` no funcionen bé quan es tracta de comparar quaternions, per tant hem definit un funció anomenada `ComparaQuaternions[p,q]` que retorna `True` si aquests són iguals i `False` si són diferents.

```
In[106]:= ComparaQuaternions[p_, q_] :=
           If[Re[p - q] == 0 && Re[Quaternion[0, 1, 0, 0] ** (p - q)] == 0 &&
             si  parte real          parte real
              Re[Quaternion[0, 0, 1, 0] ** (p - q)] == 0 &&
               parte real
              Re[Quaternion[0, 0, 0, 1] ** (p - q)] == 0, True, False]
               parte real                                  verd···  falso

In[107]:= AssociatPrimari[q_] := Module[{x}, {x} = {q};
                                  módulo
            n = 1;
            While[ComparaQuaternions[Mod[(UnitQuaternions ** q)[[n]] - 1, Quaternion[2,
             mientras                 operación módulo
                  2, 0, 0]], Quaternion[0, 0, 0, 0]] == False && ComparaQuaternions[
                                                          falso
               Mod[(UnitQuaternions ** q)[[n]] - (1 + Quaternion[1, 1, 1, 1]),
                operación módulo
                Quaternion[2, 2, 0, 0]], Quaternion[0, 0, 0, 0]] == False, n++];
                                                                      falso
            (UnitQuaternions ** q)[[n]]]
```

Per exemple, si agafem un enter de Hurwitz de coordenades no enteres, hem d'obtenir que el seu primari associat té coordenades enteres, com bé hem demostrat al llarg del treball.

```
In[108]:= a = Quaternion[1/2, 3/2, 5/2, -1/2]
          AssociatPrimari[a]

Out[108]= Quaternion[1/2, 3/2, 5/2, -1/2]

Out[109]= Quaternion[1, 0, 2, 2]

In[110]:= Mod[AssociatPrimari[a] - 1, Quaternion[2, 2, 0, 0]]
           operación módulo

Out[110]= Quaternion[0, 0, 0, 0]
```

Un altre exemple, en el que obtinguem que el primari associat al nostre enter sigui `1 + 2 ((1+i+j+k)/2)` mòdul `2(1+i)` és:

```
In[111]:= b = Quaternion[3, 9, -3, 0]
          AssociatPrimari[b]

Out[111]= Quaternion[3, 9, -3, 0]

Out[112]= Quaternion[0, -3, -9, -3]

In[113]:= Mod[AssociatPrimari[b] - (1 + Quaternion[1, 1, 1, 1]), Quaternion[2, 2, 0, 0]]
           operación módulo

Out[113]= Quaternion[0, 0, 0, 0]
```

Amb aquestes dues funcions ja podem construir l'enter primer i primari `c` tal que `p=erc`, on `e` és una unitat i `r` un nombre enter. Recordem que a la demostració del Teorema de Factorització, es busca el primer π que és el màxim comú divisor per la dreta de `c` i el factor primer més petit de la norma de `c`. La funció `FactorPrimer[q]` calcula aquest primer. L'algoritme continua de la

mateixa manera però es va dividint el quaternió `c` per l'esquerra entre els primers π que es van trobant. Aquest procés s'acaba quan la norma de l'enter que es troba és una unitat.

In[114]:=
```
FactorPrimer[q_] := RightGCD[q, FactorInteger[Norm[q]][[1]][[1]]]
                                  factoriza entero   norma
```

In[115]:=
```
FactoritzaQuaternio[q_] := Module[{x}, {x} =
                             módulo
  {QuocientEsquerra[q, Quaternion[1, 1, 0, 0]^IntegerExponent[Norm[q], 2]]};
                                                exponente entero   norma
 n =
  0;
 While[n < IntegerExponent[Norm[q], 2], Print[Quaternion[1, 1, 0, 0]]; n++];
 mientras   exponente entero   norma   escribe
 Print[QuocientDreta[x, AssociatPrimari[x]]];
 escribe
 {x} = {AssociatPrimari[x]} ;


 Print[FactorComu[x]];
 escribe
 {x} = {QuocientEsquerra[x, Quaternion [FactorComu[x], 0, 0, 0]]};
 While[Norm[x] > 1, Print[FactorPrimer[x]];
 mient···  norma   escribe
  {x} = {QuocientEsquerra[x, FactorPrimer[x]]}];
 Print[x]]
 escribe
```

Si el quaternió és parell, apareix el terme `Quaternion[1,1,0,0]` repetit tantes vegades com la potència de 2 que divideix la norma de q. Després, apareixen la unitat que passa del primari al nostre enter i el màxim comú divisor d'aquest. La resta de factors que apareixen són els quaternions primers en què descompon `q`. Vegem-ho amb alguns exemples:
Primer anem a veure la factorització d'un enter senar i primitiu.

In[116]:=
```
a = Quaternion[4, 7, -3, 1]
```

Out[116]=
```
Quaternion[4, 7, -3, 1]
```

In[117]:=
```
FactorInteger[Norm[a]]
factoriza entero   norma
```

Out[117]=
```
{{3, 1}, {5, 2}}
```

In[118]:=
```
FactoritzaQuaternio[a]
```

```
Quaternion[1, 0, 0, 0]

1

Quaternion[3/2, 1/2, -1/2, -1/2]

Quaternion[2, 0, 0, 1]

Quaternion[2, 0, 0, 1]

Quaternion[1/2, 1/2, -1/2, -1/2]
```

In[119]:=
```
Quaternion[3/2, 1/2, -1/2, -1/2] ** Quaternion[2, 0, 0, 1] **
  Quaternion[2, 0, 0, 1] ** Quaternion[1/2, 1/2, -1/2, -1/2] == a
```

Out[119]= True

Podem observar que, tal i com ens indiquen els factors primers de la norma de **a**, hem obtingut un quaternió primer de norma 3 i dos quaternions primers de norma 5. Ara veurem un exemple de quaternió parell i no primitiu.

In[120]:=
```
b = Quaternion[6, -12, 0, 0]
```

Out[120]= Quaternion[6, -12, 0, 0]

In[121]:=
```
Quaternion[6, -12, 0, 0]
```

Out[121]= Quaternion[6, -12, 0, 0]

In[122]:=
```
FactorInteger[Norm[b]]
```
factoriza entero norma

Out[122]= {{2, 2}, {3, 2}, {5, 1}}

In[123]:=
```
FactoritzaQuaternio[b]
```

```
Quaternion[1, 1, 0, 0]

Quaternion[1, 1, 0, 0]

Quaternion[0, -1, 0, 0]

3

Quaternion[2, 1, 0, 0]

Quaternion[0, -1, 0, 0]
```

In[124]:=
```
3 ** Quaternion[1, 1, 0, 0] ** Quaternion[1, 1, 0, 0] **
  Quaternion[0, -1, 0, 0] ** Quaternion[2, 1, 0, 0] ** Quaternion[0, -1, 0, 0] == b
```

Out[124]= True

En aquest cas, hem tret el 3 com a factor comú i com que el 2 divideix dues vegades a la norma de **b**, apareix dues vegades el terme **(1+i)**.

9 Conclusions

L'estudi dels enters de Hurwitz només és una petita part del que pot veure's de les àlgebres de quaternions en general i, més encara, de les àlgebres no commutatives. Al llarg del treball hem anat topant amb resultats que mostren la importància d'aquestes àlgebres. Per mostrar un exemple, una idea que m'ha sorgit un cop vist el teorema de Lagrange que hem demostrat amb els quaternions de Hurwitz és:

> *Atès que a partir d'una àlgebra simple* 4 *dimensional hem pogut trobar un ordre que té una forma nòrmica associada equivalent a la suma de quatre quadrats podríem, de la mateixa manera, trobar ordres en àlgebres simples n dimensionals i estudiar-ne les seves formes nòrmiques.*

Aquest projecte m'ha ajudat a comprendre la immensitat de camins que poden prendre's per arribar a un mateix lloc i, al mateix temps, cada camí pot arribar a esdevenir un nou resultat.

A banda de tots els coneixements adquirits, he aprofitat el fet que la principal font que he utilitzat està en alemany per familiaritzar-me amb l'idioma, que desconeixia totalment.

Referències

[1] Alsina, M.; Bayer, P. Quaternion orders, quadratic forms, and Shimura curves. CRM Monograph Series, 22. *American Mathematical Society,* Providence, RI, 2004.

[2] Artin, E. *Geometric algebra.* Reprint of the 1957 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1988.

[3] Baez, John C. The octonions. *Bull. Amer. Math. Soc.* (N.S.) 39 (2002), no. 2, 145–205.

[4] Blanchard, A. *Les corps non commutatifs.* Collection SUP. Le mathematicien. 9. Paris: Presses Universitaires de France. 136 p. F 18.00 (1972).

[5] Bogdan, Victor M. On Frobenius, Mazur, and Gelfand-Mazur theorems on division algebras. *Quaest. Math.* 29 (2006), no. 2, 171–209.

[6] Burton, David M. *Elementary number theory.* Second edition. W. C. Brown Publishers, Dubuque, IA, 1989.

[7] Davidoff, G.; Sarnak, P.; Valette, A. *Elementary number theory, group theory and Ramanujan graphs.* London Mathematical Society Student Texts. 55. Cambridge: Cambridge University Press. 144 p. (2003).

[8] Grup alternat: `https://en.wikipedia.org/wiki/Talk%3AAlternating_group`.

[9] Guerrero, E; Pérez. E. El teorema de Skolem y Noether. *Abstraction & Application* 2 (2010) 59-68.

[10] Hurwitz, A. Ueber die Zahlentheorie der Quaternionen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen*, Mathematisch-Physikalische Kl. Göttingen; 1896, 1933. *Mathematische Werke*, Band II, Birkhäuser, 1963, LXIV, p. 303–330.

[11] Hurwitz, A. *Vorlesungen über die Zahlentheorie der Quaternionen.* Berlin. Verlag von Julius Springer, 1919.

[12] Rotman, Joseph J. *An introduction to the theory of groups.* Fourth edition. Graduate Texts in Mathematics, 148. Springer-Verlag, New York, 1995.

[13] Sánchez Muñoz, J.M. Hamilton y el Descubrimiento de los Cuaterniones. Revista *Pensamiento Matemático*- Número 1 - Oct 2011.

[14] Serre, Jean-Pierre. L'invariant de Witt de la forme $Tr(x^2)$. *Comment. Math. Helv.* 59 (1984), no. 4, 651– 676.

[15] Stankewicz, J. *Quaternion algebras and modular forms.* `http://stankewicz.net/quatalg.pdf`.

[16] Torres Del Castillo, G.F. La representación de las rotaciones mediante cuaterniones. *Miscelánea Matemática.* 29 (1999).

[17] Travesa, A. *Teoria de nombres.* `https://atlas.mat.ub.edu/personals/travesa/`.

[18] Vignéras, Marie-France. *Arithmétique des algèbres de quaternions.* Lecture Notes in Mathematics, 800. Springer, Berlin, 1980.

[19] Wolfram Research, Inc. *Mathematica*. Versió 10.4 Wolfram Research, Inc. Champaign, Illinois, 2016.